Managed Threat Detection

Product Overview

Issue	08
Date	2022-10-26

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 What Is MTD?

Managed Threat Detection (MTD) continuously checks source IP addresses and domain names in cloud service logs and alert you to potential malicious activities and unauthorized behaviors. MTD can monitor logs of IAM, DNS, CTS, OBS and VPC, all of which are global services in your account.

Powered by an AI engine, threat intelligence, and detection policies, MTD intelligently examines access behavior in logs of cloud services to detect threats, generate alarms, and provide remediation. With MTD, you can respond to alarms, handle potential threats, and harden service security in a timely manner to prevent major losses such as information leakage, keeping your accounts and service secure and stable.

NOTE

MTD is to be taken offline. For details, see **Huawei Cloud Managed Threat Detection (MTD) Will Be Taken Offline**.

MTD's capabilities will be provided by **SecMaster**. To avoid any impact on your business, you are advised to submit a service ticket to switch your operations to SecMaster as soon as possible. This will ensure better support for you.

Detection Types

Table 1-1 lists the MTD detection types supported in each region.

Table 1-1 Detection types

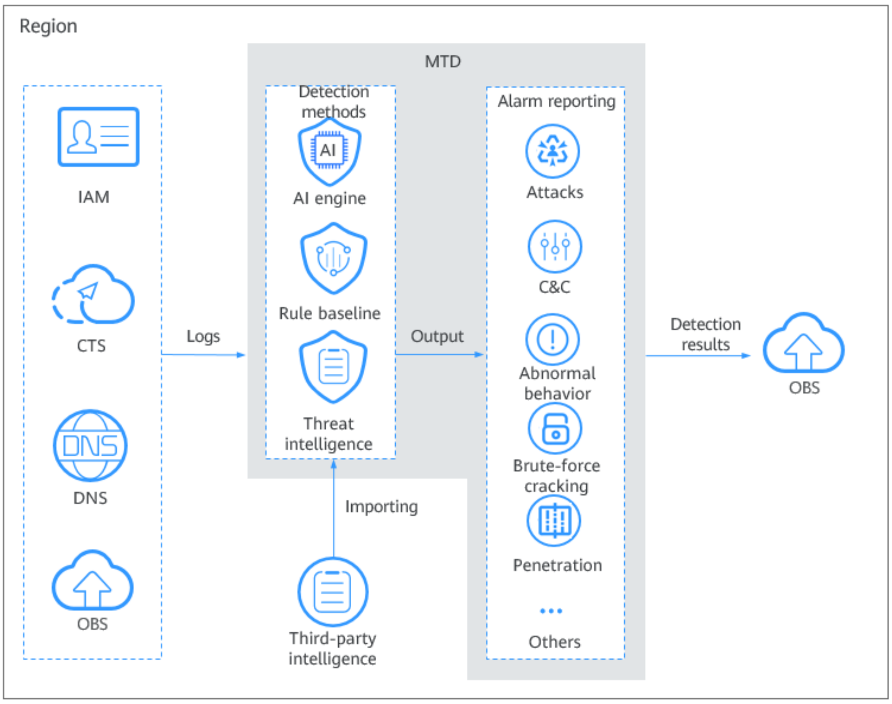
Region	IAM Detection	DNS Detection	CTS Detection	OBS Detection	VPC Detection
AP-Bangkok	√	-	√	√	√
AP-Singapore	√	√	√	√	√
LA-MexicoCity	-	-	√	-	-

Region	IAM Detection	DNS Detection	CTS Detection	OBS Detection	VPC Detection
CN-Hong Kong	√	√	-	√	-

Detection Mechanism

MTD collects logs from IAM, DNS, CTS, OBS, and VPC and uses an AI engine, threat intelligence, and detection policies to continuously detect potential threats, malicious activities, and unauthorized behaviors, such as brute-force cracking, penetration attacks, and mining attacks. **Figure 1-1** shows how MTD works.

Figure 1-1 Detection mechanism



2 Functions

AI-Powered Threat Detection

MTD introduces an AI detection engine to work together with threat intelligence and detection policies. The AI detection engine uses an elastic profile model, unsupervised model, and supervised model to detect seven high-risk scenarios of IAM, including risky passwords, credential leakage, token exploitation, abnormal delegation, remote logins, unknown threats, and brute-force cracking. It can detect abnormal behaviors using algorithms such as SVM, random forest, and neural network.

The AI detection engine keeps the model learning the real data, ensures repeated verification and manual review of the model, and accurately formulates the pre-filtering and post-processing logic. Based on the prior knowledge, the model produces zero false positives. In addition, the models are continuously optimized by retraining with detection results for a certain period of time and periodically updating dependency files, improving the model alarm accuracy.

Real-time Detection and Quick Risk Elimination

MTD obtains logs of IAM, DNS, CTS, OBS, and VPC in real time for continuous detection. MTD notifies you of detected threats once a threat is discovered, enabling you to respond to and handle the threats in a timely manner. This reduces response time and minimizes your loss.

Rating Threat Alarms by Severity

MTD grades the alarms by severity levels, including critical, high, medium, low, and informational. This helps you determine how serious an alarm is and what response you should take to minimize threat impacts.

Library Management Policy

You can upload or add intelligence or whitelist to an OBS bucket and asynchronously synchronize them to MTD. Then, MTD preferentially uses the synchronized library to detect threats, detecting new threats in a timely manner and ignoring activities from whitelisted IP addresses or domain names. This reduces the detection response time and service loads.

3 Advantages

Abnormal IAM Behavior Detection with an AI Engine

MTD introduces an AI detection engine to work together with threat intelligence and detection policies. The AI detection engine uses an elastic profile model, unsupervised model, and supervised model to detect abnormal behaviors in seven high-risk scenarios of IAM, including risky passwords, credential leakage, token exploitation, abnormal delegation, remote logins, unknown threats, and brute-force cracking.

Industry-Leading Algorithm Architecture

Based on analysis on DNS domain name characteristics and BERT concept, MTD builds a three-channel CNN model. Compared with the traditional method of directly inputting domain names to the neural network, the three-channel CNN model can detect threats faster and more accurately.

Accurate Threat Identification with Multiple Models

In addition to threat intelligence and detection policies, MTD provides three types of algorithm capabilities based on the AI engine, including IAM anomaly detection, DNS Trojan horse detection, and DNS suspicious domain name detection. For different detection targets, seven AI models are trained using algorithms such as supervised or unsupervised deep neural network and Markov. A comprehensive detection system is built based on feature rules, distribution statistics, and externally input threat intelligence, effectively improving threat analysis efficiency and accuracy.

Blacklist/Whitelist Library

MTD can aggregate historical intelligence discovered by MTD or other services in plaintext format and allow you to define the threat detection scope by adding your custom whitelist. MTD ignores the activities of IP addresses in the whitelist and generates alerts for the activities of IP addresses in the intelligence library.

Aggregation with Other Services

- MTD allows you to transfer detection results to an OBS bucket for long-term storage.

- The threat detection results of MTD can be synchronized to Situation Awareness (SA) as an important input for the follow-up security analysis and operations.

4 Application Scenarios

Checking Logs of Global Services

MTD collects logs from IAM, DNS, CTS, OBS, and VPC and uses an AI engine, threat intelligence, and detection policies to continuously detect potential threats, malicious activities, and unauthorized behaviors, such as brute-force cracking, penetration attacks, and mining attacks. You can view alarms on a graphical dashboard.

Identifying Distributed Brute-force Attacks

MTD uses an AI engine for detection, improving the detection efficiency and accuracy and being capable of detecting potential threats, which takes the lead in the industry.

The AI detection engine can detect IAM anomalies to protect your accounts. The AI detection engine uses an elastic profile model, unsupervised model, and supervised model to detect abnormal behaviors in seven high-risk scenarios of IAM, including risky passwords, credential leakage, token exploitation, abnormal delegation, remote logins, unknown threats, and brute-force cracking. Therefore, MTD can detect distributed brute-force attacks even if they occur with low frequency.

Detecting Botnets and Trojans

Based on the BERT model, MTD divides DNS into three channels (Bigram, Segment, and Position) and constructs a three-channel CNN model to detect scanning behavior and mining behavior. The model can effectively detect the Linux.Ngioweb botnet, SystemdMiner Trojans, WatchBog Trojans, and Bad Rabbit ransomware.

Data Aggregation

Third-party threat intelligence in STIX/CSV format and IP address whitelists can be imported into OBS and asynchronously synchronized to MTD. MTD then preferentially detects the IP addresses and domain names in the list library, and identifies activities related to the IP addresses and domain names in the imported intelligence or ignores activities related to the IP addresses or domain names in the imported whitelists, reducing the detection response time and service running load. In addition, detection results can be uploaded to OBS for long-term storage.

5 Basic Concepts

Detector

A detector is a region entity created once MTD is enabled in a region. All threat detection results in the region are associated with the detector.

Data Source

Data source refers to the logs of services. These logs are detected and analyzed by MTD to identify the potential threats. To identify unauthorized malicious activities, MTD must be granted the permissions for accessing the log data of target services, including IAM, DNS, CTS, OBS, and VPC.

6 Billing

MTD supports the yearly/monthly billing mode. If you choose this mode, the longer you use, the more you save.

Billing Items

You are billed based on the purchased specifications, usage duration, and the volume of scanned logs that exceeds the specifications per month.

Table 6-1 MTD billing

Billing Item	Description
(Mandatory) Edition	You are billed based on the package edition you choose, including Bronze, Silver, Gold, and Platinum packages.
Add-on package	If you finish the package quota, you will be billed based on the exceeding data volume on a pay-per-use basis. **CAUTION** You do not need to buy add-on packages. The system automatically purchases an add-on package for you based on the volume of scanned data exceeding the package quota and charges you on a pay-per-use basis.
(Mandatory) Required duration	You will be billed on a yearly or monthly basis.

Billing Mode

In yearly/monthly mode, the longer you use, the more you save. You need to pay the bill for the required duration.

Renewal

Renew your subscription in time so we can keep MTD resources such as historical alarms for you. If you do not renew the service after it expires, MTD will charge you on a pay-per-use basis.

You can go to the management console to renew your subscription. For details, see **Manual Renewal**.

Expiration and Overdue Payment

- Expiration

  If you do not renew MTD after it expires, your resources will enter a retention period. The resources will be automatically deleted and cannot be restored and the service cannot be renewed after the retention period ends. For details about the retention period, see **Resource Suspension and Release**.

  NOTE

  If the specifications you purchased expire and you do not renew them, MTD will charge you on a pay-per-use basis.

- Overdue Payment

  An **add-on package** may cause your account be in arrears.

  If this happens, you can go to the Billing Center for detailed information. To repay the bill, see **Making Repayments (Prepaid Direct Customers)**.

Helpful Links

Will I Be Charged If I Disable All Log Data Sources After Purchasing MTD?

7 Permission Management

If you need to assign different permissions to employees in your enterprise to access your MTD resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you efficiently manage access to your MTD resources.

With IAM, you can use your account to create IAM users for your employees, and assign permissions to the users to control their access to specific resource types. For example, some software developers in your enterprise need to use MTD but must not delete MTD resources or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using MTD resources.

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 the **IAM Service Overview**.

MTD Permissions

By default, new IAM users do not have any permissions. You need to add a user to one or more groups, and attach permissions policies or roles to these groups. Users inherit permissions from their owning groups and can perform specified operations on cloud services based on the permissions.

MTD 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. Users need to switch to the authorized region when accessing MTD.

You can grant users permissions by using roles and policies.

- Roles: A coarse-grained authorization mechanism provided by IAM to define permissions based on users' job responsibilities. This mechanism provides a limited number of service-level roles for authorization. If one role has a dependency role required for accessing MTD, assign both roles to the users. Roles are not an ideal choice for fine-grained authorization and secure access control.

- Policies: A 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 MTD users the permissions to manage only a certain type of resources.

8 MTD and Other Services

IAM

Identity and Access Management (IAM) provides you with permission management for MTD. Only users granted with the MTD Administrator permissions can use MTD. To obtain the permissions, contact the users who have the Security Administrator permissions. MTD detects malicious activities and unauthorized behaviors in IAM log data.

CTS

Cloud Trace Service (CTS) records operations related to MTD, facilitating your further queries, audits, and retrievals. MTD detects malicious activities and unauthorized behaviors in CTS log data.

VPC

A **Virtual Private Cloud (VPC)** is a private and isolated virtual network on Huawei Cloud. After being authorized, MTD can detect and identify the malicious attacks and unauthorized accesses in the logs of VPC.

DNS

Domain Name Service (DNS) provides DNS services and domain name management services. MTD detects malicious activities and unauthorized behavior in DNS log data.

OBS

Object Storage Service (OBS) is a stable, secure, and easy-to-use object storage service that lets you inexpensively store data of any format and size. You can enable BOS for MTD to store threat detection results to a bucket, meeting compliance requirements. For details, see **Synchronizing Detection Results**.

9 Comparison with Other Services

Differences Between MTD and SA

Situation Awareness (SA) is a UI-based security management platform for threat detection and analysis. SA focuses on the security threat attack posture of all your cloud assets. By aggregating detection results or events from many security products and analyzing threat data and cloud security threats, it helps you build a security system covering all your cloud assets.

MTD detects potential threats in your cloud services. It uses the AI engine, threat intelligence, and detection policies to detect threats in cloud service logs, generates alarms for detected threats, and displays statistics on the alarms.

Table 9-1 Differences between MTD and SA

Feature	MTD	SA
Supported product/ service	● Identity and Access Management (IAM) ● Domain Name Service (DNS) ● Cloud Trace Service (CTS) ● Virtual Private Cloud (VPC) ● Object Storage Service (OBS)	● Host Security Service (HSS) ● Anti-DDoS ● Web Application Firewall (WAF) ● Cloud Bastion Host (CBH) ● Container Guard Service (CGS) ● Vulnerability Scan Service (VSS)
Data source detection/ analysis	● IAM full logs ● DNS full logs ● CTS full logs ● Full logs of global service VPC ● OBS full logs	● Network-wide traffic ● Logs from the security defense devices ● DNS requests ● Threat intelligence ● Security Information

Feature	MTD	SA
Threat detection	● Alarms MTD can report more than 40 types of alarms for the threats detected on the basis of the AI engine, threat intelligence, and detection policies.	● Alarm events SA detects and displays eight types of alarm events, including more than 200 sub-types. SA also reports alarm notifications. ● Security orchestration SA allows you to implement preset security orchestration policies to harden asset security.

Anti-Brute-Force Cracking Differences Between MTD and HSS

Host Security Service (HSS) improves the overall security of hosts on Huawei Cloud. HSS focuses on identifying and managing information assets on your hosts, monitoring risks on your hosts in real time, preventing unauthorized intrusions, and reducing security risks on your hosts.

In addition to detecting threats based on detection policies and intelligence, MTD uses an AI-powered detection model to detect abnormal IAM activities. Additionally, the abnormal behavior detection model of MTD detects distributed brute-force attacks on IAM accounts.

Table 9-2 Differences between MTD and HSS

Feature	MTD	Host Security Service (HSS)
Object	● All accounts of your services	● SSH account ● RDP account ● FTP account ● SQL Server account ● MySQL account ● Other accounts

Feature	MTD	Host Security Service (HSS)
Brute-force attacks	● MTD allows you to import threat intelligence and a whitelist to set the detection scope. It ignores the activities of whitelisted IP addresses and reports alarms for access from IP addresses or domain names that are similar to historical intelligence. ● MTD reports alarms when a user attempts to log in to the system within IAM lock time, or when a user logs in to the system or obtains the token across regions.	● If the number of brute-force attacks from an IP address reaches 5 within 30 seconds, the IP address will be blocked. ● You can check whether the IP address is trustworthy based on its attack type and how many times it has been blocked. You can manually unblock the IP addresses you trust.
Abnormal login	● MTD reports alarms if login or token obtaining success rate changes abruptly or the total number of logins or token obtaining increases sharply. ● MTD reports an alarm if an IP address attempts to log in or obtain a token for the first time. ● MTD reports an alarm if an IP address is used for remote login.	● HSS detects remote logins to your hosts and reports alarms. HSS checks the blocked login IP addresses, and who used them to log in to which servers at what time. ● HSS reports an alarm if a user's login location is not any common login location. ● Trigger an alarm if a user logs in to the host by a brute-force attack.

Feature	MTD	Host Security Service (HSS)
Abnormal behavior	● MTD identifies distributed brute-force attacks. MTD can effectively detect continuous attacks on IAM accounts using random public IP addresses through HTTP tunnels. Each attacking IP address is used for less than three times. These distributed brute-force attacks cannot be detected by conventional security system. ● MTD detects AK/SK leakage. ● MTD detects malicious agency. ● MTD detects suspicious malicious use of tokens. ● MTD detects suspicious password cracking behavior.	● HSS monitors abnormal CPU usage. ● HSS monitors malicious IP addresses accessing processes ● HSS monitors abnormal increase in concurrent process connections

A Change History

Date	Description
2022-10-26	This issue is the eighth official release. Updated **Billing** and added the description of the billing mode for each package.
2022-06-14	This issue is the seventh official release. Added section **Billing**.
2022-04-26	This issue is the sixth official release. Added the **CN-Hong Kong** region. IAM, DNS, CTS, OBS, and VPC detection is supported in the **CN-Hong Kong** region.
2022-03-28	This issue is the fifth official release. Provisioned DNS detection for AP-Bangkok, and IAM, DNS, CTS, OBS, and VPC detection for AP-Singapore.
2022-03-08	This issue is the fourth official release. Modified **What Is MTD?**
2022-01-14	This issue is the third official release. Added VPC threat detection and optimized the description.
2021-11-17	This issue is the second official release. Added fine-grained authorization and modified **Permission Management**.
2021-10-12	This issue is the first official release.