

Managed Threat Detection

Getting Started

Issue 09
Date 2022-12-02



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

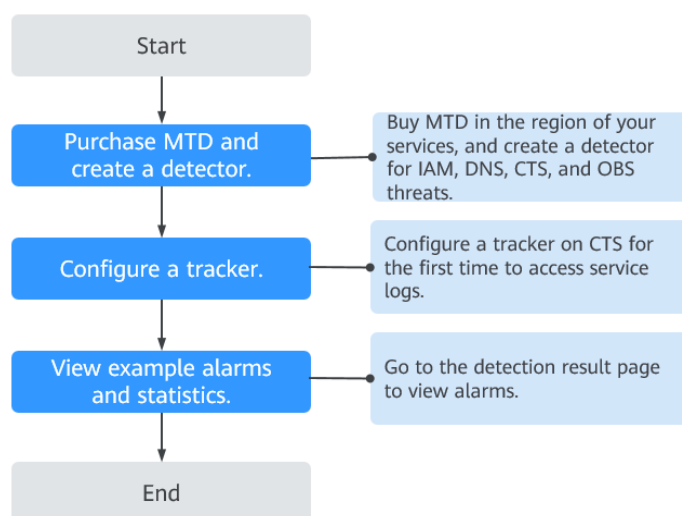
Contents

1 Process.....	1
1.1 Step 1: Purchase MTD and Create a Detector.....	1
1.2 Step 2: Create a Tracker.....	5
2 Example Alarms and Statistics.....	8
2.1 IAM Alarms.....	8
2.2 CTS Alarms.....	15
2.3 DNS Alarms.....	17
2.4 OBS Alarms.....	20
2.5 VPC Alarms.....	23
A Change History.....	27

1 Process

On the Huawei Cloud management console, purchase MTD, create a detector, and configure a tracker so that MTD can obtain service logs. [Figure 1-1](#) shows the process.

Figure 1-1 Process to use MTD



1.1 Step 1: Purchase MTD and Create a Detector

MTD uses a detector to scan service logs in the target region in real time.

Prerequisites

MTD permissions have been granted to a user of the IAM account. For details, see [How Do I Use My IAM Account to Grant MTD Permissions to a User?](#)

NOTICE

To create a detector and then perform other operations, you need to obtain permissions from the IAM account first.

Otherwise, you cannot perform operations on MTD.

If you are an administrator, perform the following operations to grant required permissions to the user:

1. Create a custom policy.

Create a custom policy on the IAM console. For details, see [Creating a Custom Policy](#).

2. Create a user group and grant permissions to the user group.


Grant policy permissions to the group where the user belongs. For details, see [Creating a User Group and Assigning Permissions](#).

Constraints

- Currently, MTD is supported in **AP-Bangkok**, **AP-Singapore**, **LA-MexicoCity1**, **LA-Sao Paulo1**, **CN-Hong Kong**, **AF-Johannesburg**, and **LA-Santiago** regions only.
- You can create a detector only in the region where your cloud services locate.

Procedure

Step 1 [Log in to the management console](#).

Step 2 Click  in the upper left corner of the management console and select a region or project.


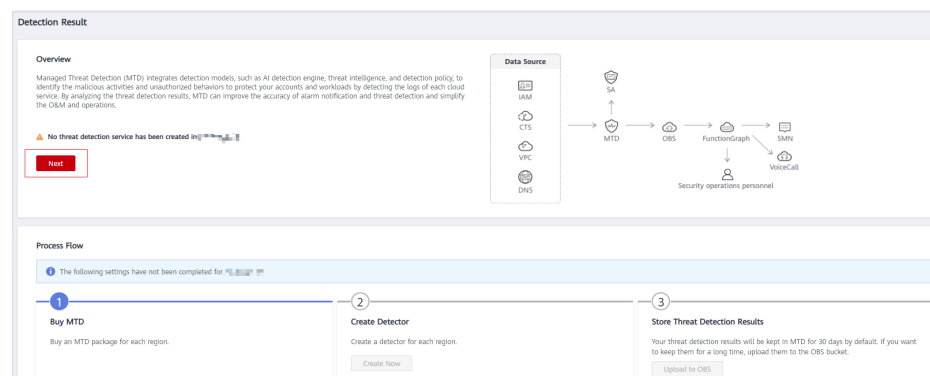
Step 3 Click  in the navigation pane on the left and choose **Security & Compliance > Managed Threat Detection**.

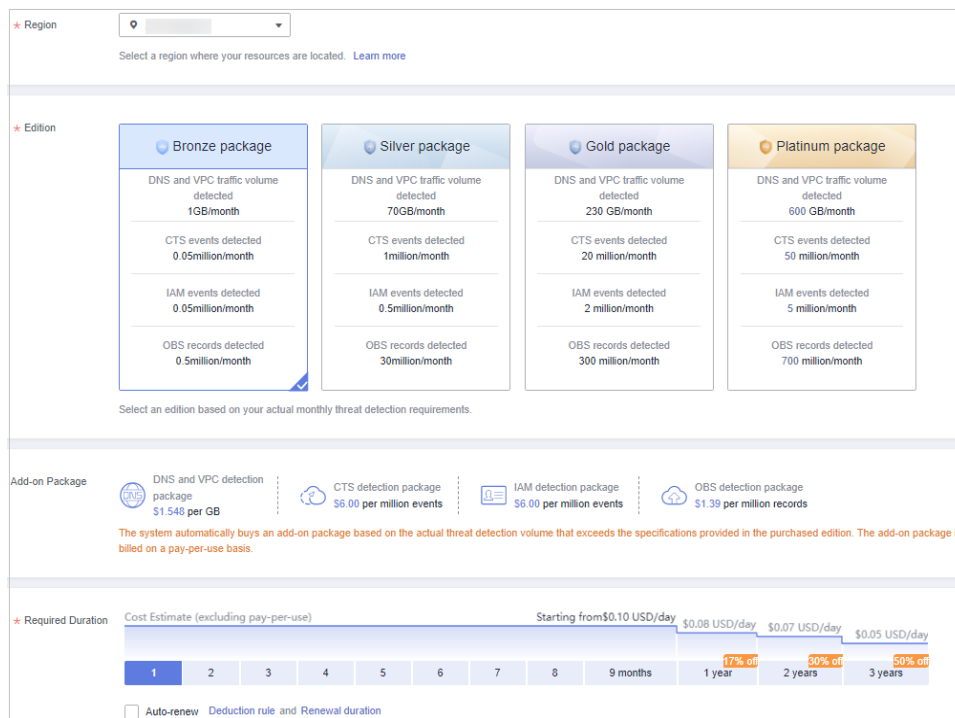
Figure 1-2 Home page of MTD



Step 4 Click **Create Now**. The purchase details page is displayed.

Step 5 On the displayed page, set the **Region**, **Edition**, and **Required Duration** as needed.

Figure 1-3 Purchasing MTD



1. Specify the **Region**.

Select the desired region. MTD cannot be used across regions.

2. Select the **Edition**.

There are four detection packages you can choose from. Each package allows you to scan different volumes of cloud service logs. For details, see [Specifications](#). DNS and VPC service logs are counted by data volume, and CTS, IAM, and OBS service logs are counted by event (one log is an event).

Table 1-1 Specifications

Edition	DNS and VPC Logs	CTS Logs	IAM Logs	OBS Logs
Bronze package	1 GB/month	50 thousand/month	50 thousand/month	500 thousand/month
Silver package	70 GB/month	1 million/month	500 thousand/month	30 million/month
Gold package	230 GB/month	20 million/month	2 million/month	300 million/month
Platinum package	600 GB/month	50 million/month	5 million/month	700 million/month

3. Choose an **Add-on Package**.

The system automatically purchases an add-on package based on the volume of scanned data that exceeds the purchased package. The add-on package is billed on a pay-per-use basis.

4. Specify the **Required Duration**.

The required duration can be from one month to three years.

NOTICE

- For archiving purposes, you are advised to buy at least three months of the service.

- You can enable **Auto-renew** after specifying the required duration.

Deduction rule: The renewal charges are automatically deducted from your account balance. For details, see [Auto-Renewal Rules](#).

Renewal duration: For a monthly subscription, the system renews the package on a monthly basis. For a yearly subscription, the system renews the package on a yearly basis.

Step 6 Read and select *Managed Threat Detection Service Disclaimer* and *Add-on Pack Usage Rules*.

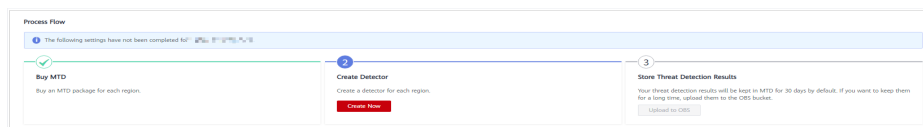
Step 7 Click **Create Now** in the lower right corner to continue on the confirmation page.

Step 8 Confirm the purchase information and click **Pay Now** in the lower right corner. The **Pay** page is displayed.

Step 9 Select a payment method and complete the payment. **Payment processed successfully** is displayed.

Step 10 Click **Back to Console** to switch to the MTD management console. On the **Detection Result** page, view the **Process Flow**. If **Buy MTD** is checked as shown in [Figure 1-4](#), the purchase is successful. You then need to create a detector in the current region.

Figure 1-4 MTD successfully purchased




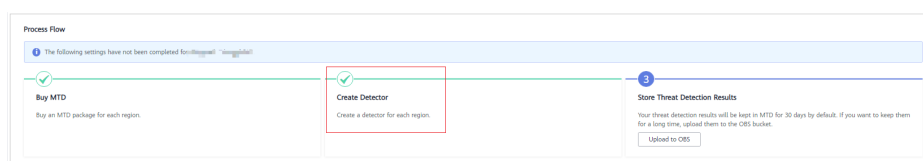
Step 11 Click **Create Now** in the **Create Detector** pane. After the creation is complete, **Detector created** is displayed. The page is automatically refreshed. Click  in the upper left corner of the page to show the **Process Flow**. If **Create Detector** is checked as shown in [Figure 1-5](#), the detector is successfully created. The purchased package is displayed in the upper right corner of the page.

Figure 1-5 Detector created successfully



 NOTE

The detection function is enabled for logs of all supported services by default after you create the detector for the first time.

----End

1.2 Step 2: Create a Tracker

After you create the detector, CTS threat detection is enabled by default. However, MTD cannot obtain log data from the CTS service without a tracker.


This section describes how to configure the tracker.


Limitations and Constraints

CTS threat detection is not supported for the **CN-Hong Kong** region.

Procedure

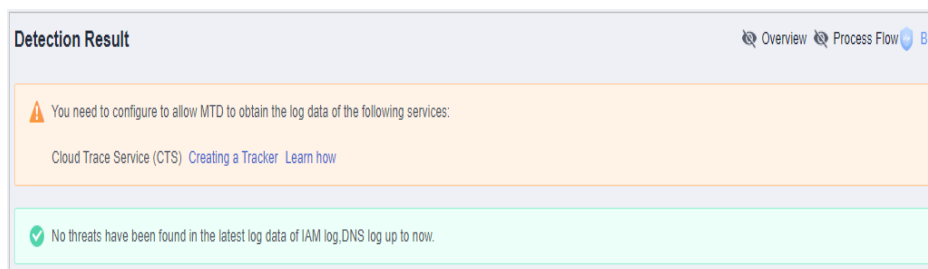
Step 1 [Log in to the management console.](#)

Step 2 Click  in the upper left corner of the management console and select a region or project.

Step 3 Click  in the left navigation pane and choose **Security & Compliance > Managed Threat Detection**.

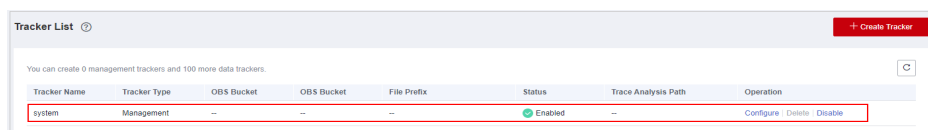
View the notice on the **Detection Result** page.

Figure 1-6 Notice on the detection result page



Step 4 Click **Creating a Tracker** to switch to the CTS **Tracker List** page. In the tracker list, locate the only default tracker which is of the **Management** type.

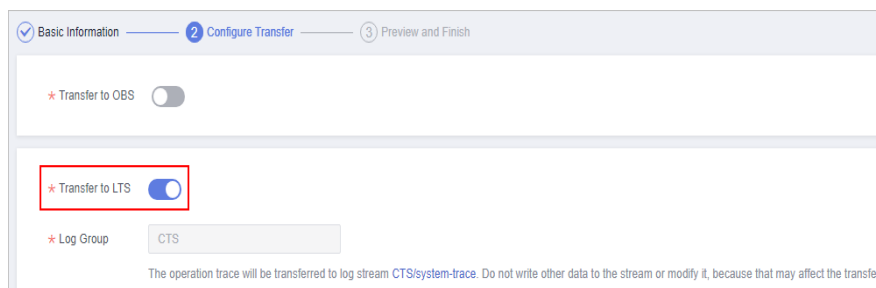
Figure 1-7 Management tracker



Step 5 In the row that contains the target tracker, click **Configure** in the **Operation** column.

1. On the **Basic Information** page, the tracker name is generated by default.
2. Click **Next** to go to the **Configure Transfer** page.
3. On the **Configure Transfer** page, toggle on **Transfer to LTS**.

Figure 1-8 Configure Transfer



4. Click **Next** to go to the **Preview and Finish** page
5. Confirm settings and click **Configure**.

Step 6 Go back to the MTD console.


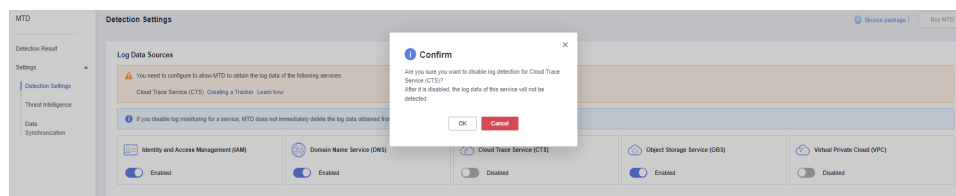
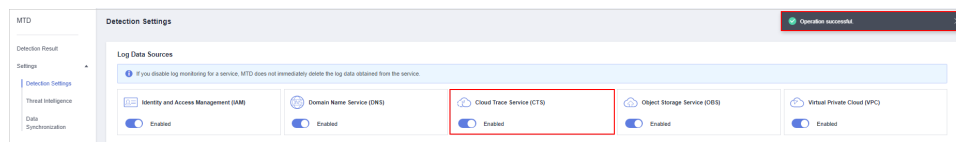
Step 7 In the left navigation pane, choose **Settings > Detection Settings**. On the **Detection Settings** page, click  next to **Cloud Trace Service (CTS)** to turn the toggle off. In the displayed dialog box, click **OK** to temporarily disable CTS threat detection. **Operation successfully!** is displayed in the upper right corner.

Figure 1-9 Disabling CTS



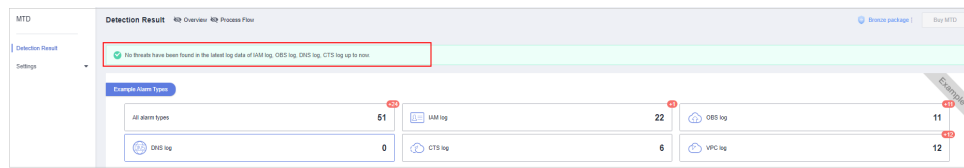
Step 8 Click  next to **Cloud Trace Service Log (CTS)** to enable CTS threat detection. **Operation successfully!** is displayed in the upper right corner.

Figure 1-10 Enabling CTS



Step 9 In the navigation pane on the left, choose **Detection Result**. On the displayed page, "No threats have been found in the latest log data of IAM log, OBS log, DNS log, CTS log up to now" disappears. If CTS threat detection is enabled, the tracker is configured successfully.

Figure 1-11 Tracker configured



----End

2 Example Alarms and Statistics

2.1 IAM Alarms

Attacker

Access from an attacker's IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BlackList

Access from a blacklisted IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

CnC

A CnC IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Compromised

A compromised IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Crawler

A crawler's IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

DDoS

A DDoS IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Exploit

An IP address used for vulnerability exploitation is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

MaliciousSite

Access through the destination IP addresses of a malicious site is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Malware

Access from a malware's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Miner

Access from a miner's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

MiningPool

Access through the destination IP addresses of a mining pool is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Payment

Access through the destination IP addresses of a fraudulent payment website is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Phishing

Access from a phishing website's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Proxy

Access from a malicious agency's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Scanner

Access from a malicious scanner's IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

SinkHole

Access from a sinkhole IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Spammer

Access from a spammer IP address is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Suspicious

Access to a suspicious IP address that is similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Tor

A Tor node IP address similar to historical intelligence is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Zombie

Access from a malicious website/zombie network is detected.

Severity: medium

Data source: IAM logs

A malicious IP address similar to historical intelligence has been found accessing the IAM account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

Bruteforce

Brute-force password cracking attempts are detected.

Severity: medium

Data source: IAM logs

This IAM account may have been cracked. Check whether this account has weak passwords or password leak risks.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BruteforceSuccess

The password may have been successfully cracked through brute-force attacks.

Severity: high

Data source: IAM logs

The IAM account may have been cracked and the password may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

AkSkLeakage

There is a risk of AK/SK credential leak.

Severity: medium

Data source: IAM logs

The AK of this IAM account may be exploited. Check whether the AK and SK of this account is leaked.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

AkSkLeakageSuccess

The AK/SK credential may have been disclosed.

Severity: high

Data source: IAM logs

The AK and SK of this IAM account may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BlindIpLogin

An unauthorized IP address is detected trying to log in to this IAM account.

Severity: medium

Data source: IAM logs

The IAM account is being used for multiple login attempts through an unauthorized IP address. Check whether this account has a weak password or whether the password has been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

BlindIpLoginSuccess

An unauthorized IP address has been used to log in to this IAM account.

Severity: high

Data source: IAM logs

The IAM account has been logged in through an unauthorized IP address. The password may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

IllegalAssume

The IAM account is detected trying to create a malicious agency.

Severity: medium

Data source: IAM logs

The IAM account may be involved in activities related to malicious agencies.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

IllegalAssumeSuccess

The IAM account has been used to successfully create a malicious agency.

Severity: high

Data source: IAM logs

The IAM account may have established a malicious agency.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

TokenLeakage

There is a risk that the token is used maliciously.

Severity: medium

Data source: IAM logs

The IAM account is at risk of token exploitation. Check whether the token is disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

TokenLeakageSuccess

The token has been used maliciously.

Severity: high

Data source: IAM logs

The token of this IAM account has been used maliciously. The token may have been disclosed.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

2.2 CTS Alarms

NetworkPermissions

A malicious IP address similar to historical intelligence is found calling an API that is typically used to change permission of network access to security groups, routes, and ACLs in your account.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is typically used to change permission of network access to security groups, routes, and ACLs in your account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

ResourcePermissions

A malicious IP address similar to historical intelligence is found calling an API that is typically used to change secure access policies for various resources in your account.

Severity: This alarm can be of any severity levels within **High, Medium, and Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is typically used to change secure access policies for various resources in your account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

UserPermissions

A malicious IP address similar to historical intelligence is found calling an API that is typically used to add, modify, or delete IAM users, groups, or policies in your account.

Severity: This alarm can be of any severity levels within **High, Medium, and Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is typically used to add, modify, or delete IAM users, groups, or policies in your account.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

ComputeResources

A malicious IP address similar to historical intelligence is found calling an API that is typically used to start compute resources, such as ECS instances.

Severity: This alarm can be of any severity levels within **High, Medium, and Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to call an API that is usually used to start computing resources, such as ECS instances.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

PasswordPolicyChange

A malicious IP address similar historical intelligence is found trying to change the account password policy.

Severity: This alarm can be of any severity levels within **High**, **Medium**, and **Low**. MTD determines the potential risk the finding could have to your network.

Data source: CTS logs

A malicious IP address similar to historical intelligence is detected. The IP address tried to change the account password policy.

Suggestions

If this is an expected activity, add the IP address to the whitelist.

2.3 DNS Alarms

Adware

Access to adware is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a malicious adware similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

CnC

Access to a CnC server is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a CnC server similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Exploit

Access to a domain name that exploits system vulnerabilities is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a domain name similar to historical intelligence, which may exploit system vulnerabilities.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

MaliciousSite

Access to a malicious website is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a malicious website that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Malware

Access to malware is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed malware that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Miner

Access to a miner is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a miner that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

MiningPool

Access to a mining pool is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a mining pool that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Payment

Access to a payment domain name is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a payment domain name that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Phishing

Access to a phishing website is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a phishing website that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Spammer

Access to a spammer is detected.

Severity: medium

Data source: DNS logs

Your ECS accessed a spammer that is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

Suspicious

Suspicious access is detected.

Severity: medium

Data source: DNS logs

The ECS access is similar to historical intelligence.

Suggestions

If this is an expected activity, add the IP address of the ECS to the whitelist.

2.4 OBS Alarms

UserFirstAccess

A specific user accessed an OBS bucket for the first time.

Severity: low

Data source: OBS logs

A user who has never accessed the bucket before accessed it.

Suggestions

If the user is not authorized, credentials may have been disclosed or OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

IPFirstAccess

A specific IP address was used for the first time to access an OBS bucket.

Severity: low

Data source: OBS logs

An IP address that has never accessed the bucket before accessed it.

Suggestions

If the IP address is not authorized, credentials may have been disclosed or OBS permission is not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket, or enable OBS URL validation with the Referer added to the blacklist.

ClientFirstAccess

A new client was used to access an OBS bucket.

Severity: low

Data source: OBS logs

A client that has never accessed the bucket before accessed it.

Suggestions

If the login client is not commonly used, remediate the access policy of the compromised OBS bucket or enable OBS URL validation with the Referer added to the blacklist.

UserFirstCrossDomainAccess

An OBS instance is being accessed for the first time by a user who does not belong to your account.

Severity: low

Data source: OBS logs

A user who does not belong to your account accessed the bucket. The user client has never accessed the bucket before.

Suggestions

If the user is not authorized, credentials may have been disclosed or OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UserAccessFrequencyAbnormal

A user accessed a specific OBS bucket frequently.

Severity: low

Data source: OBS logs

Access frequency of a user that belongs to your account to the bucket is abnormal.

Suggestions

If this activity is unexpected, your OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

IPAccessFrequencyAbnormal

An IP address was used to access a specific OBS bucket frequently.

Severity: low

Data source: OBS logs

The access frequency of this IP address to the bucket is abnormal.

Suggestions

If this activity is unexpected, your OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UserDownloadAbnormal

Abnormal download behavior is detected.

Severity: low

Data source: OBS logs

The download volume from the bucket is abnormal.

Suggestions

If this activity is unexpected, the user credential may have been disclosed or the OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UserIPDownloadAbnormal

An IP address is detected in a user's abnormal download behavior.

Severity: low

Data source: OBS logs

The download volume from the bucket through the specific IP address is abnormal.

Suggestions

If this activity is unexpected, user credentials may have been disclosed or OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket.

UnauthorizedAccess

Unauthorized access is detected.

Severity: low

Data source: OBS logs

Multiple unauthorized API calls on the bucket occurred during a specific period.

Suggestions

If the activity is authorized, add the permission to the access policy for the user. If the activity is unauthorized, enable OBS URL validation with the Referer added to the blacklist.

UserHourLevelAccessAbnormal

Abnormal hourly access is detected.

Severity: low

Data source: OBS logs

API calling frequency of the bucket is abnormal in the same period of every day.

Suggestions

If this activity is unexpected, remediate the access policy of the compromised OBS bucket.

IPSwitchAbnormal

Abnormal IP address switch is detected.

Severity: low

Data source: OBS logs

The bucket is accessed by multiple IP addresses during a specific period. The number of IP addresses used is inconsistent with the number in your historical behavior.

Suggestions

If this activity is unexpected, your OBS permissions are not restrictive enough. In this case, remediate the access policy of the compromised OBS bucket, or enable OBS URL validation with the Referer added to the blacklist.

2.5 VPC Alarms

DDoSTcpDns

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the DNS protocol. The port number is 53.

Severity: high

Data source: VPC flow logs

Some ECSs may be performing DoS attacks using the DNS protocol. The port number is 53.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether the processes on port 53 are abnormal and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoSTcp

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the TCP protocol. As a result, a large volume of inbound/outbound TCP traffic is generated.

Severity: high

Data source: VPC flow logs

Some ECSs may have been used to perform Denial of Service (DoS) attacks using the TCP protocol. As a result, a large volume of inbound/outbound TCP traffic is generated.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoSUdp

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the UDP protocol. As a result, a large volume of inbound/outbound UDP traffic is generated.

Severity: high

Data source: VPC flow logs

Some ECSs may have been used to perform Denial of Service (DoS) attacks using the UDP protocol. As a result, a large volume of inbound/outbound UDP traffic is generated.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoS tcp2udp

Your ECSs may have been used to perform Denial of Service (DoS) attacks using the UDP protocol on a TCP port. For example, port 80 usually used for TCP communications is found used for UDP communications at a specific time point. As a result, a large volume of inbound/outbound UDP traffic is generated.

Severity: high

Data source: VPC flow logs

Some ECSs may be performing a DoS attack using the UDP protocol on a TCP port. For example, port 80 usually used for TCP communications is found used for UDP communications at a specific time point. As a result, a large volume of inbound/outbound UDP traffic is generated.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

DDoS Unusual Protocol

Your ECSs may have been used to perform Denial of Service (DoS) attacks using an unusual protocol. Unusual protocols are those except TCP, UDP, ICMP, IPv4, IPv6 and STP protocols.

Severity: high

Data source: VPC flow logs

Some ECSs may be performing a DoS attack using an unusual protocol. Unusual protocols are those except TCP, UDP, ICMP, IPv4, IPv6 and STP protocols.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

JunkMail

Your ECSs are communicating with remote hosts through port 25 and sending junk mails.

Severity: medium

Data source: VPC flow logs

Some ECSs are communicating with remote hosts through port 25 and sending junk mails.

Suggestions: If this activity is unexpected, your ECS may be compromised. Check whether port 25 is enabled. If necessary, disable port 25 in the security group and clear any detected malware.

UnusualNetworkPort

Your ECSs are using abnormal ports to communicate with remote hosts and may be engaged in malicious activities. The abnormal port may be any custom open port.

Severity: medium

Data source: VPC flow logs

Some ECSs are using abnormal ports to communicate with remote hosts and may be engaged in malicious activities. The abnormal port may be any custom open port.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

UnusualTrafficFlow

Your ECSs are generating a large volume of outbound traffic that deviates from the normal baseline and is all directed to the remote host.

Severity: medium

Data source: VPC flow logs

Some ECSs are generating a large volume of outbound traffic that deviates from the normal baseline and is all directed to the remote host.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

Cryptomining

Your ECSs are accessing IP addresses that are associated with crypto-mining-related activity and may be engaged in illegal activities.

Severity: high

Data source: VPC flow logs

Some ECSs are accessing IP addresses that are associated with crypto-mining-related activity and may be engaged in illegal activities.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

CommandControlActivity

Your ECS is used to send messages to a high-risk network.

Severity: high

Data source: VPC flow logs

The IP address of the ECS is querying an IP address that is associated with a known command and control server.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

PortDetection

Your ECS is probing a port on a large number of IP addresses.

Severity: high

Data source: VPC flow logs

Some ECSs are scanning ports that are active on a large number of IP addresses. The ECSs may have been compromised for slow remote port scan attacks.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

PortScan

Your ECS is scanning a port on a large number of IP addresses.

Severity: medium

Data source: VPC flow logs

Some ECSs are scanning the outbound ports of remote resources and may be engaged in malicious activities.

Suggestions: If this activity is unexpected, your ECS may have been compromised. Check whether suspicious processes exist and clear any detected malware. If necessary, stop the ECS and start a new ECS to take over the workloads.

A Change History

Date	Description
2022-12-02	This issue is the ninth official release. Updated Step 1: Purchase MTD and Create a Detector : MTD is supported in the LA-Santiago region.
2022-10-26	This issue is the eighth official release. Optimized Step 1: Purchase MTD and Create a Detector .
2022-09-08	This issue is the seventh official release. Added the AF-Johannesburg region.
2022-08-10	This issue is the sixth official release. Added the LA-Sao Paulo region.
2022-04-26	This issue is the fifth official release. Added the CN-Hong Kong region.
2022-03-28	This issue is the fourth official release. Added the AP-Singapore region.
2022-01-14	This issue is the third official release. Bronze and silver packages became available for AP-Bangkok and LA-MexicoCity regions. Added VPC threat detection and optimized the description. Added Step 1: Purchase MTD and Create a Detector and Step 2: Create a Tracker to Process . Modified Example Alarms and Statistics .
2021-12-13	This issue is the second official release. Modified Example Alarms and Statistics .
2021-11-17	This issue is the first official release.