Malware Protection in Amazon Guard Duty

**Contents**

[Scope 2](#_Toc115190395)

[Problem Statement 2](#_Toc115190396)

[Introduction 3](#_Toc115190397)

[Understanding how it works 3](#_Toc115190398)

[Configure Malware Protection in standalone account 4](#_Toc115190399)

[Configure Malware Protection in multiple account environment 5](#_Toc115190400)

[Configure Malware Protection for newly added account 7](#_Toc115190401)

[Implementation 9](#_Toc115190402)

[Services Protected by GuardDuty 19](#_Toc115190402)

[Advantages 20](#_Toc115190402)

[Limitations 20](#_Toc115190413)

Malware Protection in Amazon Guard Duty

Document Name: Malware Protection in Amazon GuardDuty

Owner: Hema Paul

**Scope**

GuardDuty identifies your resources that have already been compromised by malware, or those resources that are at risk. Malware Protection supports GuardDuty to detect the malware that may be the source of this compromise.

**Problem Statement**

GuardDuty Malware Protection scans and detects malware on EBS volumes attached to your potentially compromised Amazon EC2 instances and container workloads. GuardDuty informs you of the status of your AWS environment by producing security [findings](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings.html) that you can view in the GuardDuty console or through [Amazon CloudWatch events](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings_cloudwatch.html).

**Introduction**

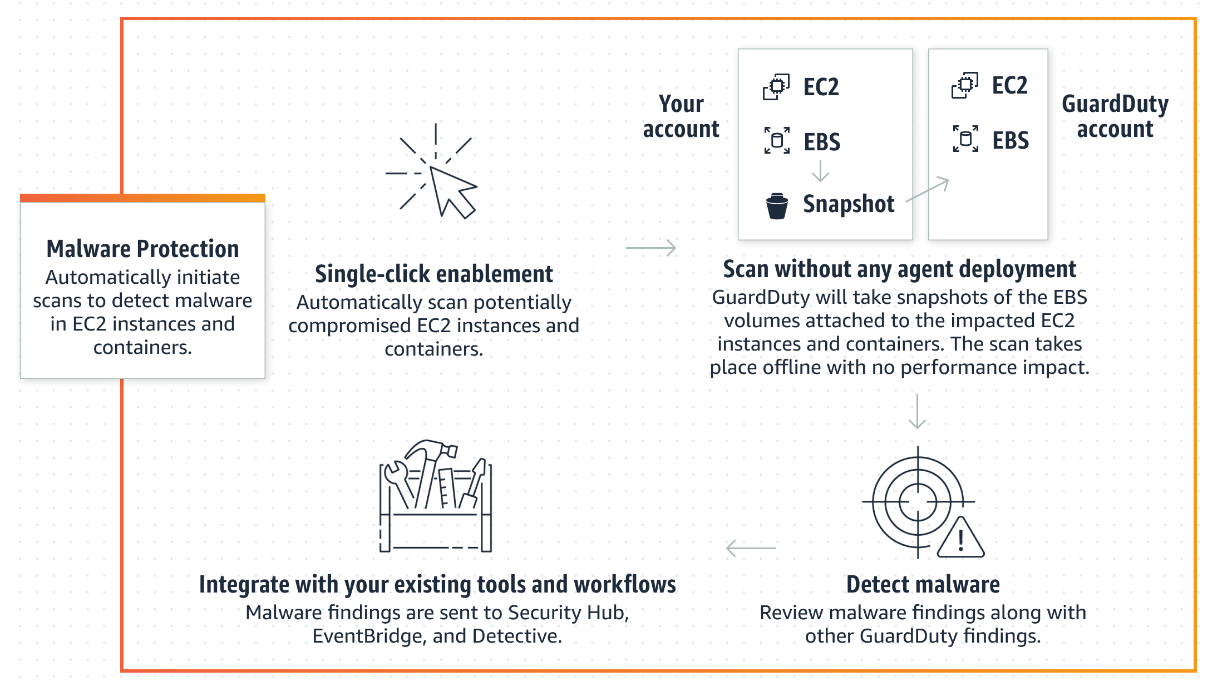
Amazon GuardDuty is a continuous security monitoring service that analyzes and processes [data sources](https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html), such as AWS CloudTrail data events for Amazon S3 logs, CloudTrail management event logs, DNS logs, Amazon EBS volume data, Amazon EKS audit logs, and Amazon VPC flow logs. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected, potentially unauthorized, and malicious activity within your AWS environment. This can include issues like escalation of privileges, use of exposed credentials, or communication with malicious IP addresses, domains, or presence of malware on your Amazon EC2 instances and container workloads. For example, GuardDuty can detect compromised EC2 instances and container workloads serving malware, or mining bitcoin. It also monitors AWS account access behavior for signs of compromise, such as unauthorized infrastructure deployments, like instances deployed in a Region that has never been used, or unusual API calls like a password policy change to reduce password strength.

With Malware Protection enabled, whenever GuardDuty detects suspicious behavior on Amazon EC2 instance or a container workload, GuardDuty Malware Protection automatically initiates an agentless scan on the Amazon Elastic Block Store (EBS) volumes attached to the impacted EC2 instance or container workload to detect the presence of malware. For more information, see [GuardDuty findings that initiate Malware Protection scans](https://docs.aws.amazon.com/guardduty/latest/ug/gd-findings-initiate-malware-protection-scan.html). GuardDuty Malware Protection also allows you to select which resources to scan or skip. GuardDuty Malware Protection may not initiate an automatic scan on the resources that you choose to exclude from scanning. If the scan detects malware, you can view the detailed Malware Protection findings about the threat in the GuardDuty console.

Malware Protection is an optional capability, and is designed to not affect the performance of your resources. Malware Protection is currently available in AWS Regions where GuardDuty is available, excluding AWS GovCloud (US) and China Regions. You can choose to start or stop Malware Protection feature for any account or available AWS Regions, at any time. By default, an existing GuardDuty customer can enable Malware Protection with a 30-day trial period. For a new GuardDuty account, Malware Protection is already enabled and included in the 30-day trial period.

## **Understanding how Malware Protection works in GuardDuty**

GuardDuty Malware Protection scans and detects malware on EBS volumes attached to your potentially compromised Amazon EC2 instances and container workloads. The following image describes how Malware Protection works in GuardDuty.



In response to GuardDuty detecting suspicious and potentially malicious activity indicative of malware, Malware Protection creates snapshots of the relevant EBS volumes attached to the resources where GuardDuty detected such activity, and shares them with the Malware Protection service account. Next, Malware Protection creates encrypted replica EBS volumes from those snapshots, in the service account.

Based on your scan option, an automatic agentless scan initiates to detect malware. After the scan completes, GuardDuty deletes the encrypted replica EBS volumes and the snapshots of your EBS volumes. If malware is found and you've turned on the snapshot retention setting, the snapshots of your EBS volumes won't get deleted and are automatically retained in your AWS account. When no malware is found, the snapshots of your EBS volumes will not be retained, irrespective of the snapshots retention setting.

GuardDuty will retain each replica EBS volume that it scans for up to one day, unless and to the extent that there is a service outage or failure with a replica EBS volume and its malware scan, at which point, GuardDuty will retain such an EBS volume for no more than seven days. The extended volume retention period is to triage and address the outage or failure. GuardDuty Malware Protection will delete the replica EBS volumes after the outage or failure is addressed or once the extended retention period lapses.

# **Configure GuardDuty Malware Protection for a standalone account**

For accounts associated with AWS Organizations, you can automate this process through console settings, as described in the next section.

Accounts that were using GuardDuty before the addition of Malware Protection can enable this feature by configuring GuardDuty through the console.

**To enable or disable Malware Protection**

Choose your access method below for instructions on enabling and disabling Malware Protection for a standalone account.

1. Open the GuardDuty console at <https://console.aws.amazon.com/guardduty/>.
2. In the navigation pane, under Settings, choose Malware Protection.
3. The Malware Protection pane lists the current status of Malware Protection for your account. You may enable or disable it at any time by selecting Enable or Disable respectively, then confirming your selection.

# **Configuring GuardDuty Malware Protection in multiple-account environments**

In a multi-account environment, only GuardDuty administrator accounts can configure Malware Protection. GuardDuty administrator accounts can enable or disable the use of Malware Protection for their member accounts. Once the administrator configures GuardDuty Malware Protection for a member account, the member account will follow the administrator account settings and be unable to modify these settings through the console. GuardDuty administrator accounts that manage their member accounts with AWS Organizations support can choose to have Malware Protection enabled automatically on all the existing and new accounts in the organization.

**Establishing trusted access to enable Malware Protection**

If the GuardDuty delegated administrator is not the same as management account in your organization, the management account must enable Malware Protection feature for their organization. This way, the delegated administrator can create the [Service-linked role permissions for GuardDuty Malware Protection](https://docs.aws.amazon.com/guardduty/latest/ug/slr-permissions-malware-protection.html) in member accounts that are managed through AWS Organizations. Choose your access method to allow GuardDuty delegated administrator to enable Malware Protection for member accounts.

1. Open the GuardDuty console at <https://console.aws.amazon.com/guardduty/>.  
   To log in, use the management account for your AWS Organizations organization.
2. In the navigation pane, choose Settings.
3. a. If you have not designated a delegated administrator, then:  
   On the Settings page, under Delegated Administrator, enter the 12-digit **account ID** that you want to designate to administer the GuardDuty policy in your organization. Choose Delegate.

b. i. If you've already designated a delegated administrator that is different from the management account, then:  
On the Settings page, under Delegated Administrator, turn on the Permissions setting. This action will allow the delegated administrator to attach relevant permissions to the member accounts and enable Malware Protection in these member accounts.

ii. If you've already designated a delegated administrator that is the same as the management account, then you can directly enable Malware Protection for the member accounts.

1. If you want to allow delegated administrators to enable Malware Protection for member accounts in other Regions, change your AWS Region, and repeat the steps above.

## **Automatically enabling Malware Protection for all organization member accounts:**

You can enable GuardDuty Malware Protection for all member accounts in an organization.

1. Open the GuardDuty console at <https://console.aws.amazon.com/guardduty/>.
2. In the navigation pane, under Settings, choose Malware Protection.
3. GuardDuty Malware Protection lists the current status of GuardDuty Malware Protection for the administrator account and the member accounts.
4. Choose Enable to start the Malware Protection service on the administrator account.
5. Choose Enable all to enable Malware Protection on all member accounts with a single click, and confirm your selection. The console will then display the number of member accounts that were enabled successfully.  
   Once enabled, you can manage member accounts from Accounts in the left navigation pane.

## **Selectively enable or disable GuardDuty Malware Protection for member accounts:**

Choose your access method below for instructions on selectively enabling and disabling Malware Protection for member accounts.

1. Open the GuardDuty console at <https://console.aws.amazon.com/guardduty/>.
2. In the navigation pane, under Settings, choose Accounts.
3. Choose the account for which you want to configure Malware Protection. From the Actions menu, choose Enable Malware Protection or Disable Malware Protection, then confirm your selection to change the settings for the selected account. The table will update automatically to show your changes.

## **Configuring Malware Protection for newly added accounts in the Organization:**

The newly added member accounts must Enable GuardDuty before selecting Enable or Disable Malware Protection.

The member accounts managed by invitation can configure GuardDuty Malware Protection manually for their accounts. Choose your access method below for instructions on how to view the current status of Malware Protection for your account.

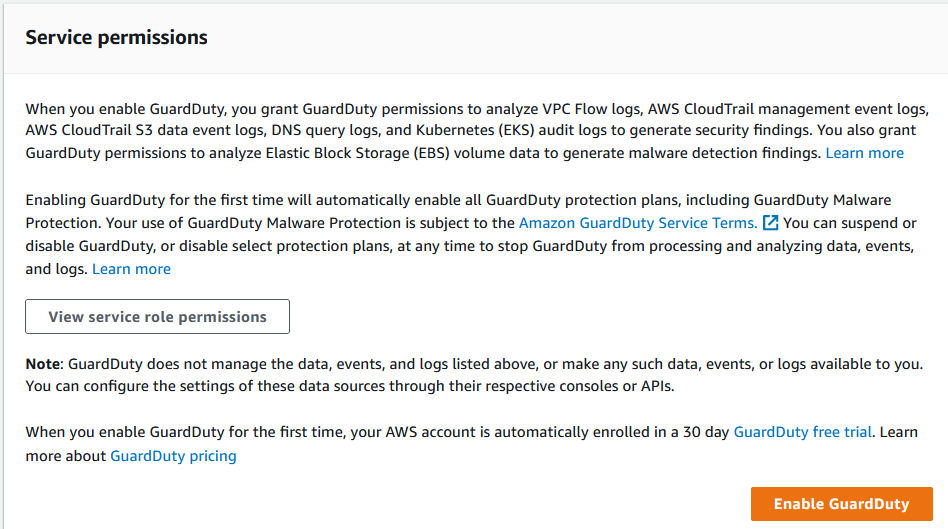
1. Open the GuardDuty console at <https://console.aws.amazon.com/guardduty/>.
2. In the navigation pane, under Settings, choose Accounts.
3. Choose Auto-enable and review the status of Malware Protection.
4. You can Enable or Disable Malware Protection for new member accounts.
5. Choose Update Settings to confirm your selection.

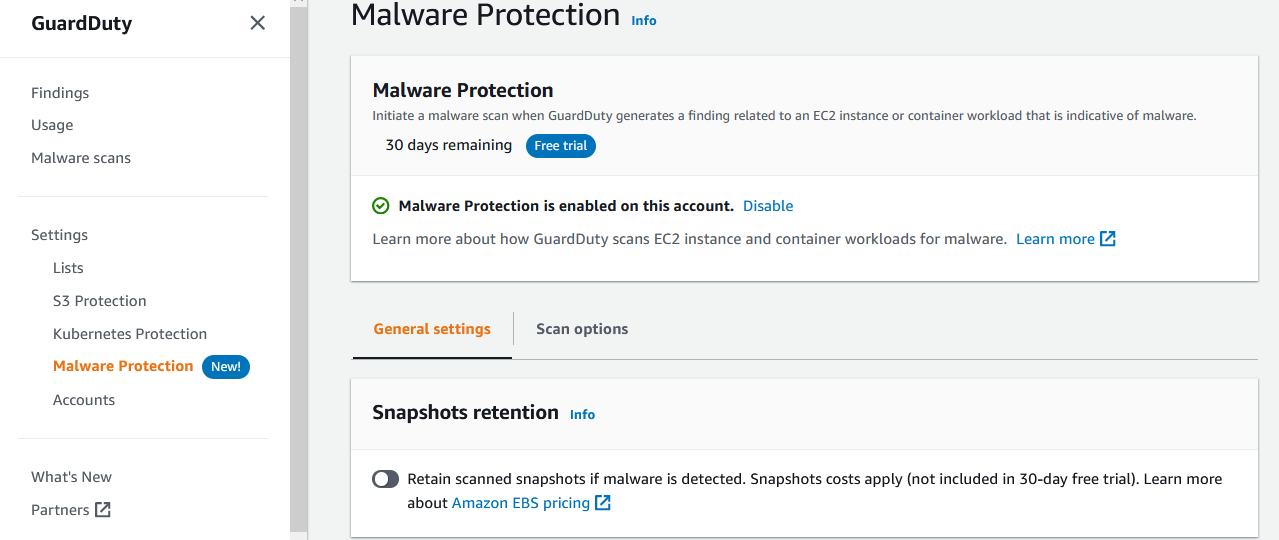
# **Enable Malware Protection for existing accounts in the Organization managed via invitation:**

The GuardDuty Malware Protection service-linked role (SLR) must be created in member accounts. The administrator can't enable the Malware Protection feature in member accounts that are not managed by AWS Organizations.

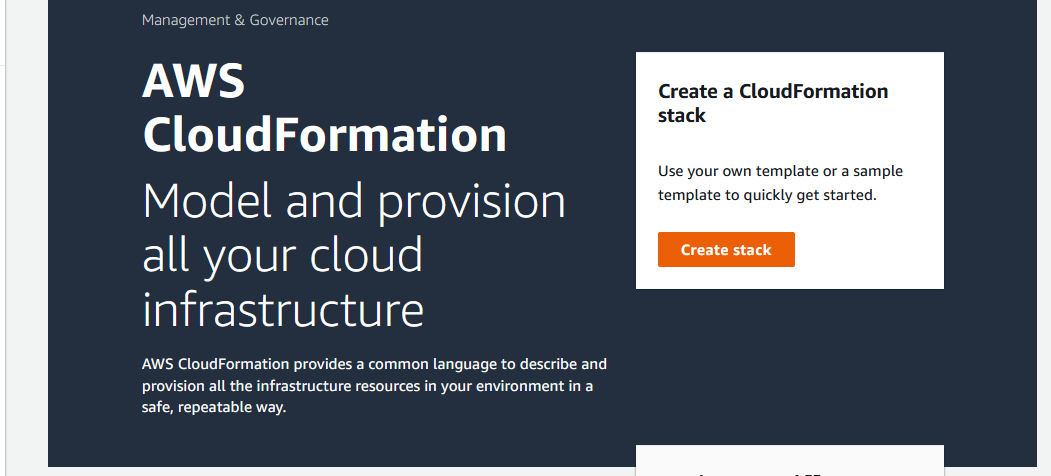
1. Open the GuardDuty console at <https://console.aws.amazon.com/guardduty/>.
2. In your administrator account, choose Accounts in the navigation pane.
3. Choose the member account that wants to enable Malware Protection and then, choose Actions.
4. Choose Disassociate member.
5. In your member account, choose Malware Protection under Settings on the navigation pane.
6. Choose Enable Malware Protection. GuardDuty will create an SLR for the member account. For more information on SLR, see [Service-linked role permissions for GuardDuty Malware Protection](https://docs.aws.amazon.com/guardduty/latest/ug/slr-permissions-malware-protection.html).
7. In your administrator account, choose Accounts under Settings on the navigation pane.
8. Choose the member account that needs to be added back to the organization.
9. Choose Actions and then, choose Add member.

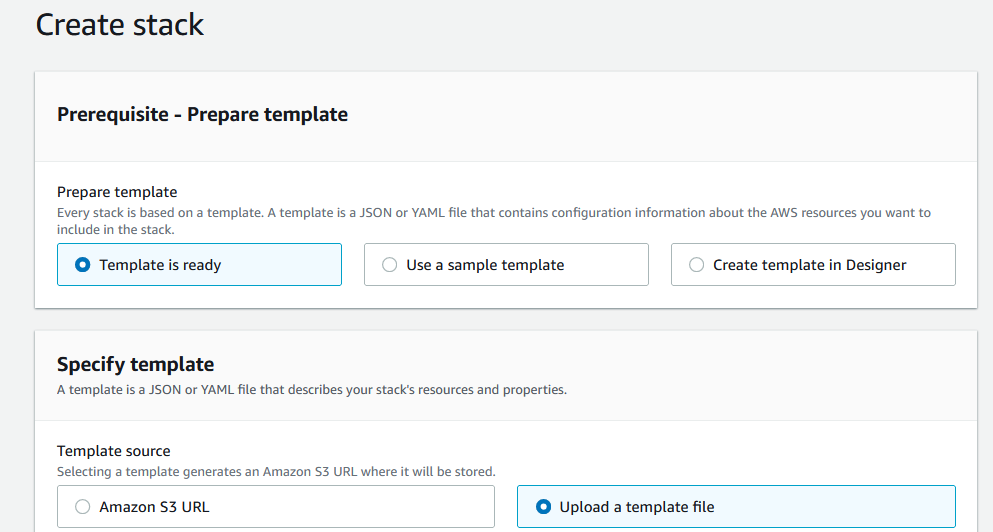
**Implementation**





After enabling GuardDuty, go to CloudFormation and create a stack.

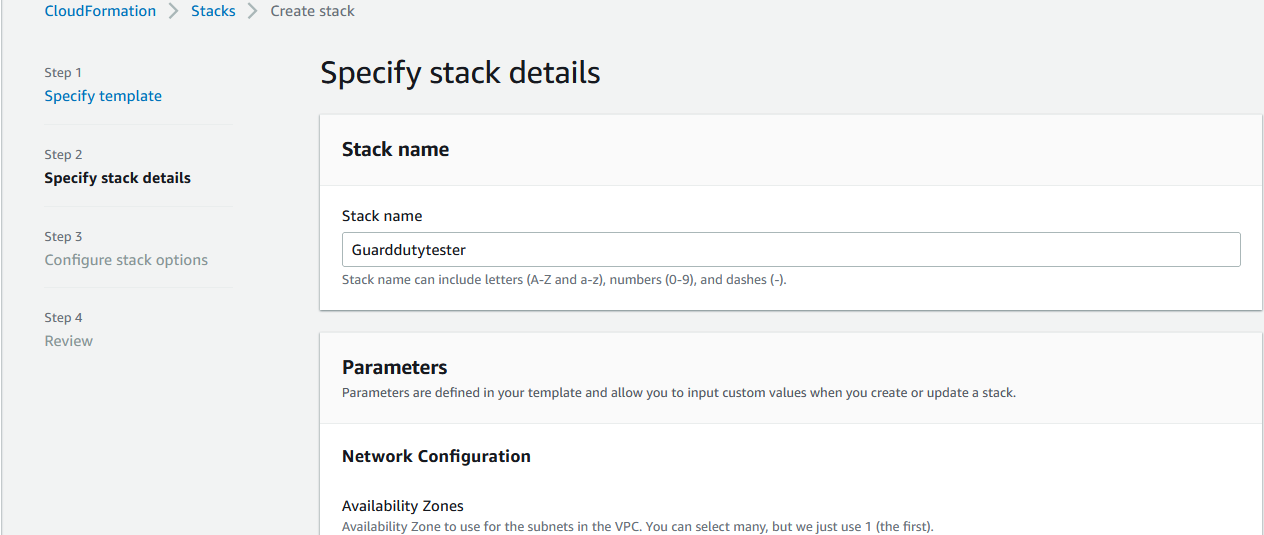




\* <https://github.com/awslabs/amazon-guardduty-tester/blob/master/guardduty-tester.template>

Download the template file from repository and save in JSON or YAML format.

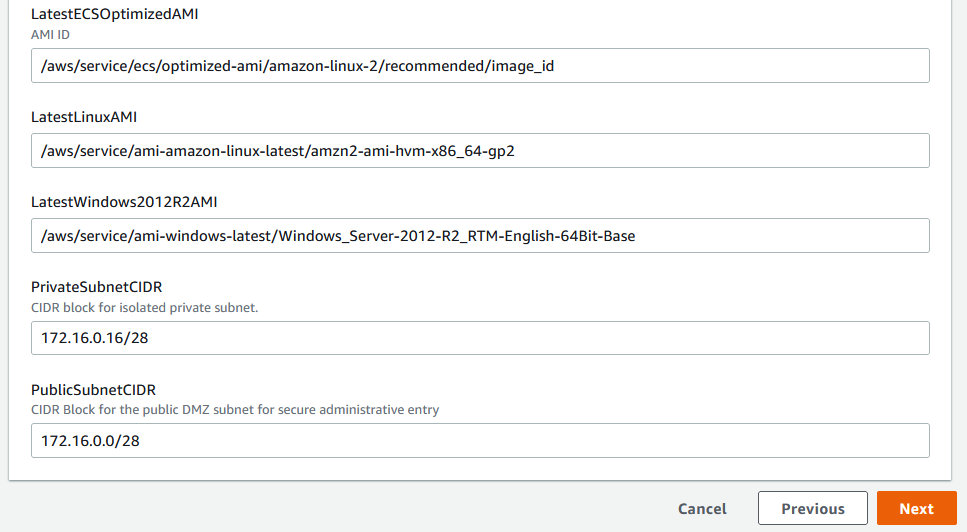
Note : This template creates the basic VPC infrastructure for an isolated testing environment. It will deploy a bastion host into the public subnet for a single Availability Zone so we have a protected point of entry. It will then create a linux instance with some red team scripts & tools that operate against common applications that are created in the same private subnet. \*\*WARNING\*\* This template creates Amazon EC2 instance and related resources. You will be billed for the AWS resources used if you create a stack from this template



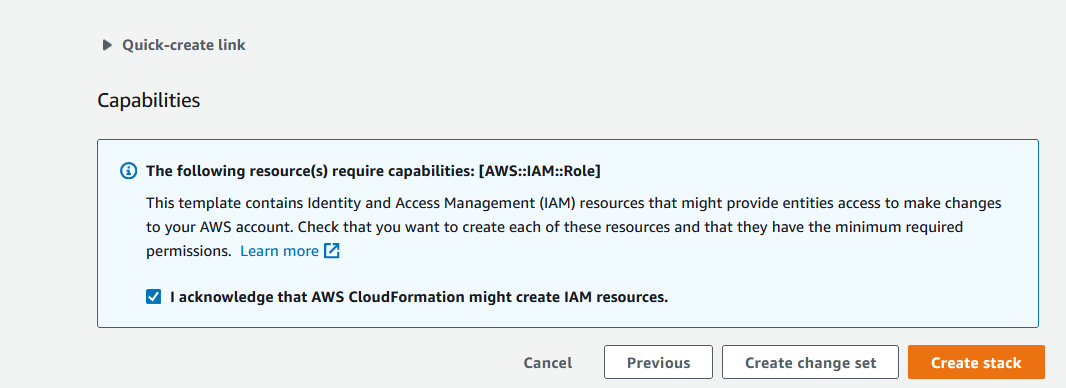
Select availability zone and choose a keypair.

Set rest of the options are as default.

Click next.

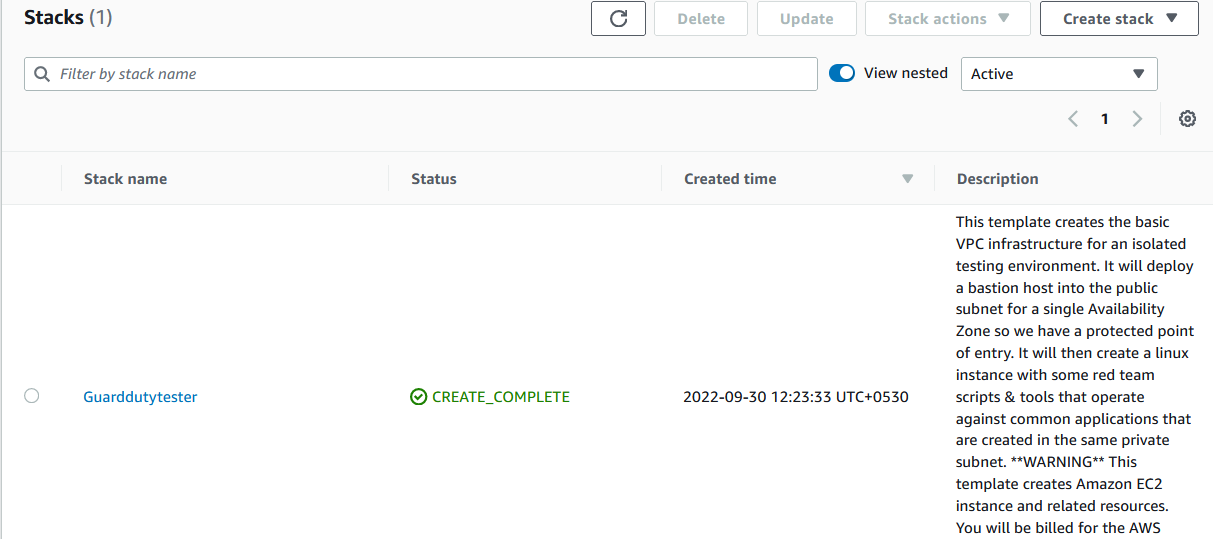


In the quick create link check the acknowledge text and click create stack

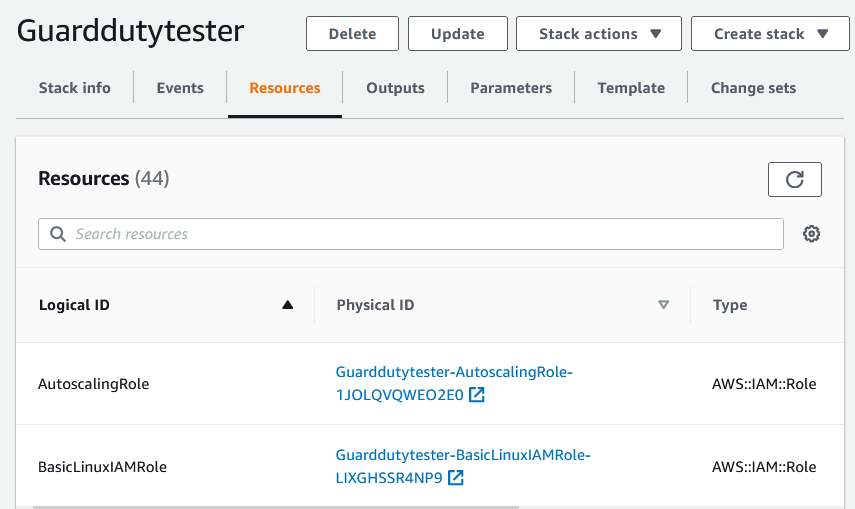


Creating stack will take about 10 to 15 minutes.

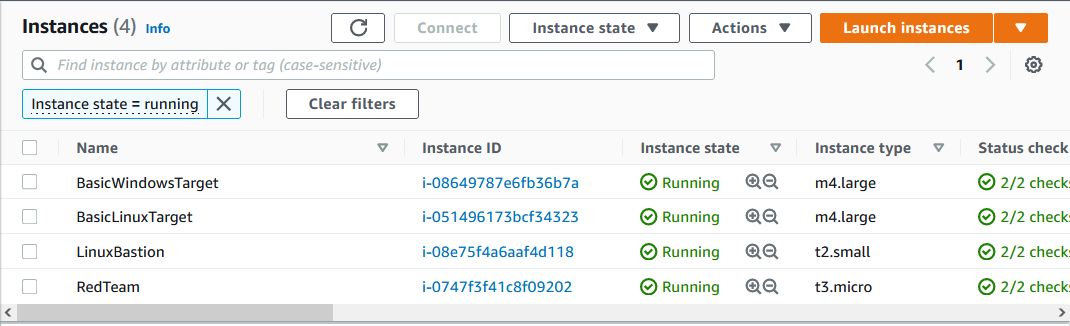
Successfully created stack.



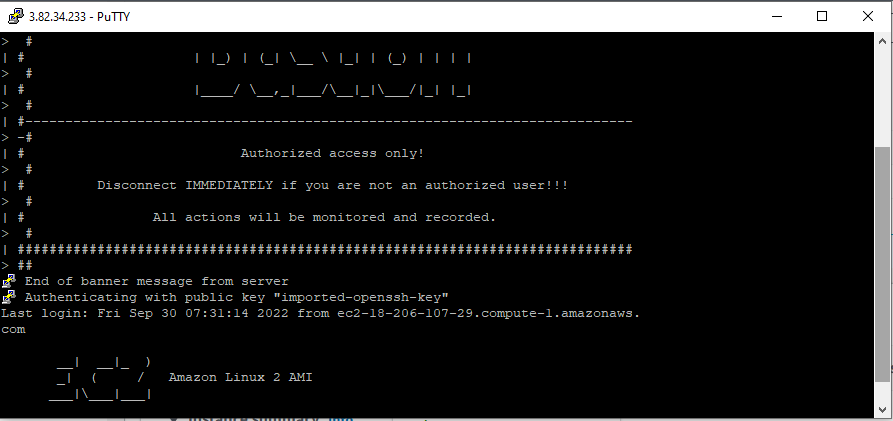
Looking in the Resources tab , we can see number of resources are created.



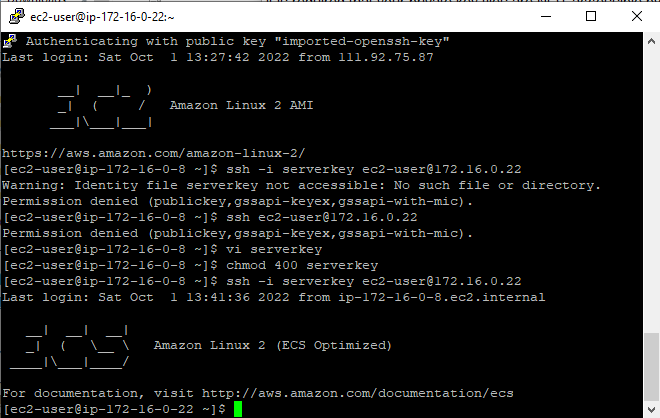
Now go to the EC2 instances ,where we can see the running instances created.



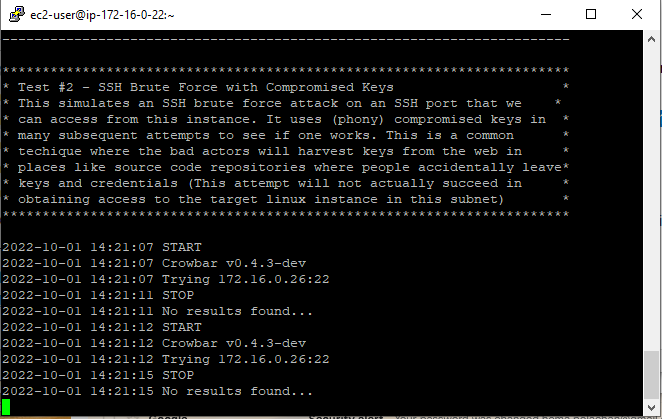
Connect the LinuxBastion instance to SSH via putty

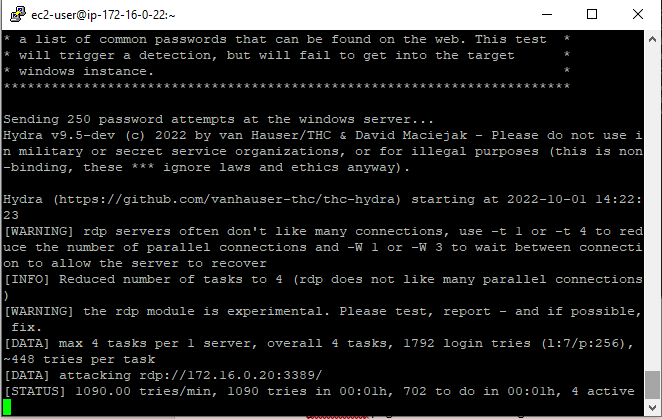


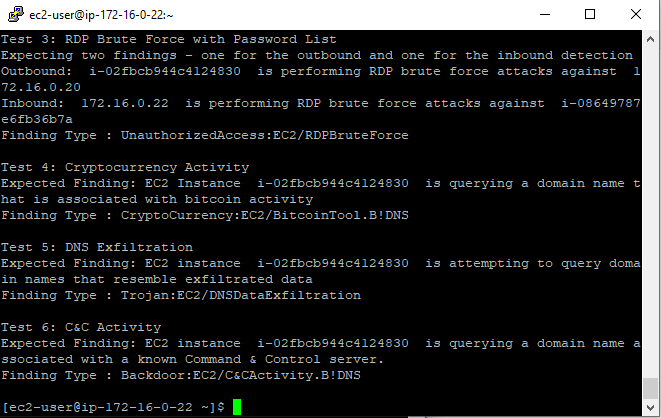
Connect RedTeam instance



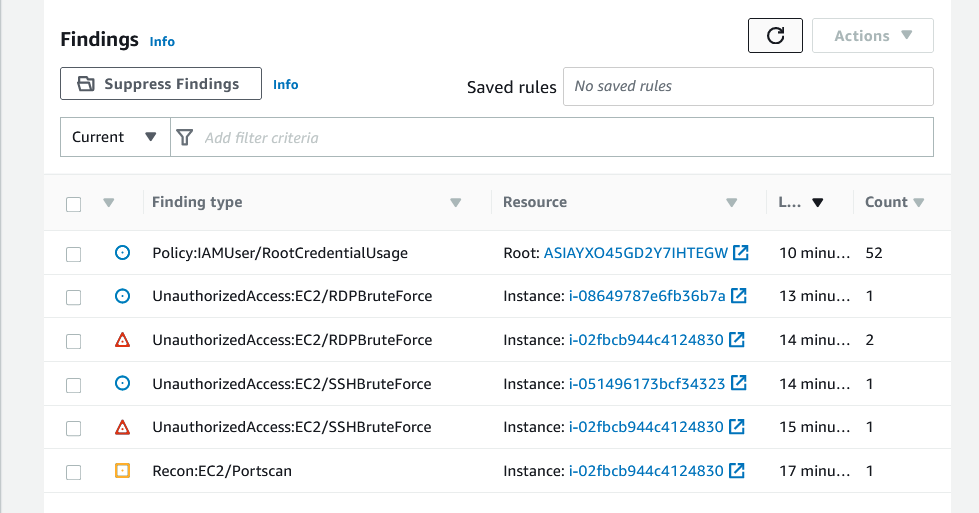
Run command ./guardduty\_tester.sh to simulate malware



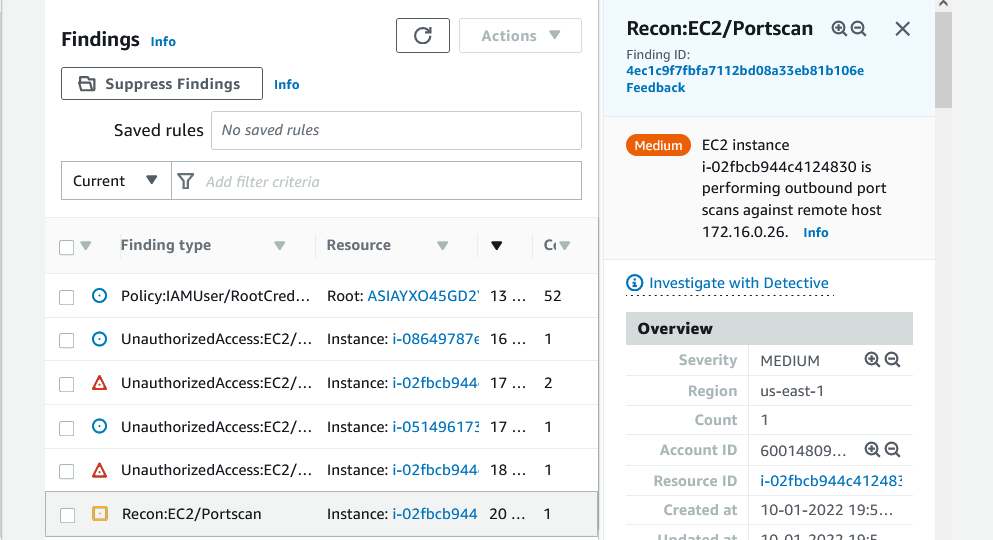




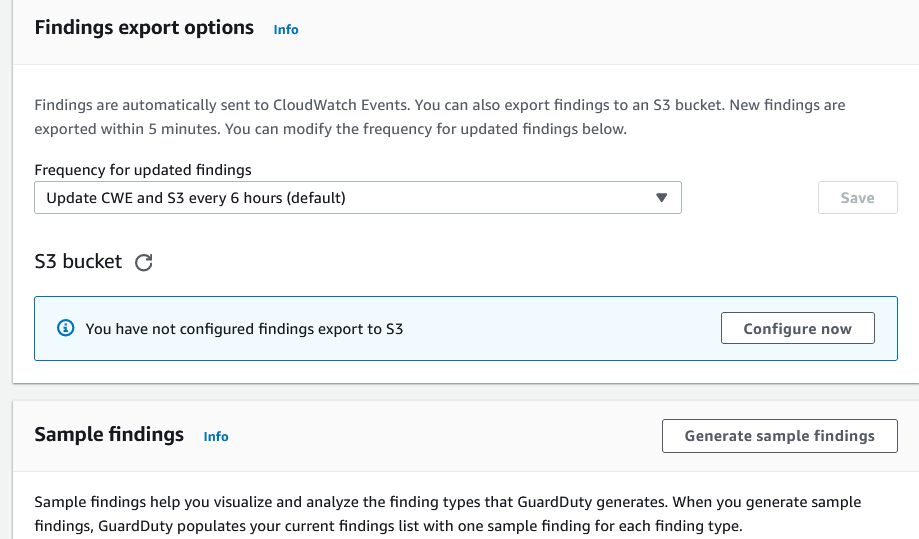
Now go to view the findings in guardduty .



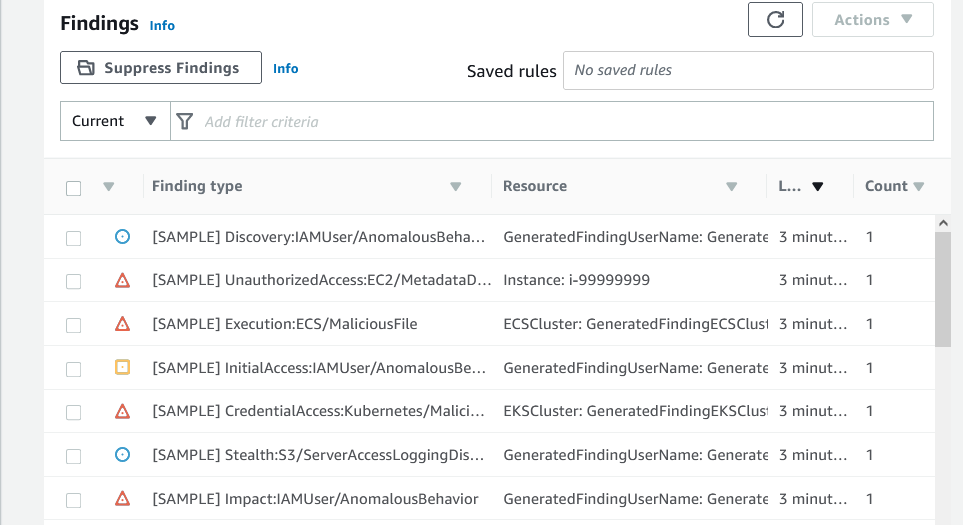
Upon clicking on the each finding, it will show the details



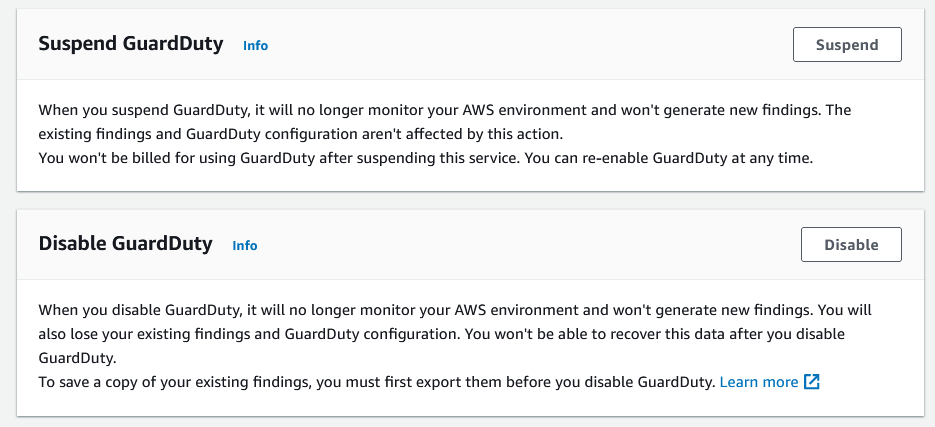
There is option to export the logs to s3 bucket or to local



If we generate sample findings that also will get listed in the findings

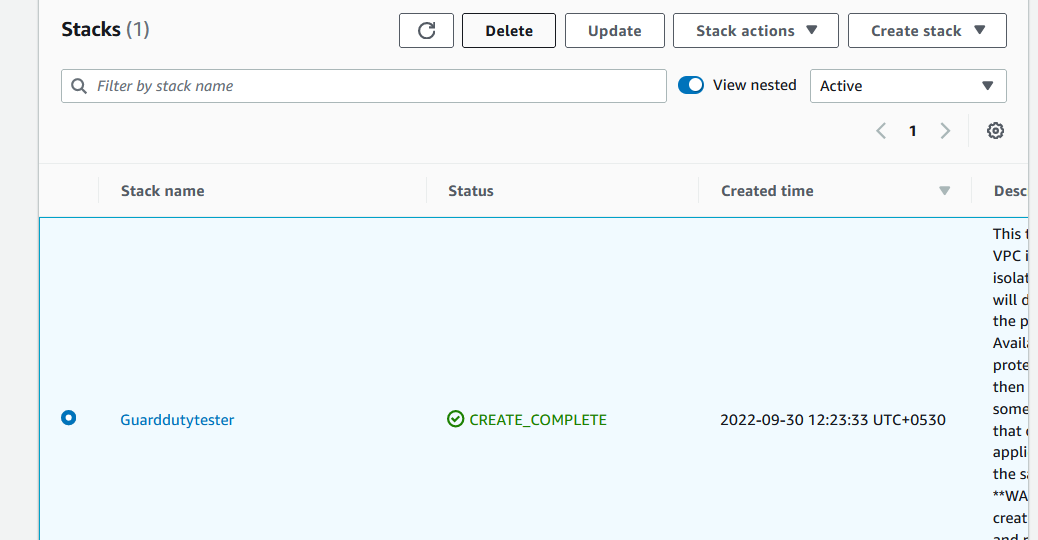


There are Suspend and Disable options in guard duty.

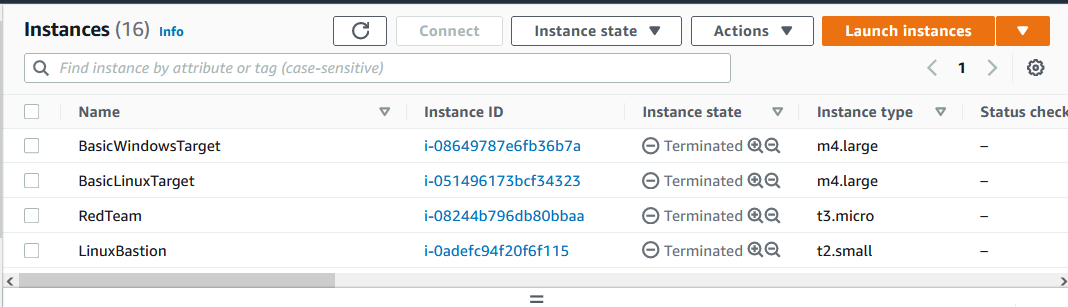


Finally delete the guardduty created

Choose the stack name and click Delete.



On deleting the stack , the instances also will get terminated.



**Services Protected by GuardDuty**

GuardDuty is an intelligent threat detection service that continuously monitors your AWS accounts, Amazon Elastic Compute Cloud (EC2) instances, Amazon Elastic Kubernetes Service (EKS) clusters, and data stored in Amazon Simple Storage Service (S3) for malicious activity without the use of security software or agents.

**EC2 Protection**

Once the feature is enabled, GuardDuty **Malware Protection** will initiate a malware scan in response to relevant EC2 findings. You don't have to deploy any agents, there are no log sources to enable, and there are no other configuration changes to make.

**S3 Bucket Protection**

S3 protection enables Amazon GuardDuty to monitor object-level API operations to identify potential security risks for data within your S3 buckets.

GuardDuty monitors threats against your Amazon S3 resources by analyzing AWS CloudTrail management events and CloudTrail S3 data events. These data sources monitor different kinds of activity, for example, CloudTrail management events for S3 include operations that list or configure S3 buckets.

GuardDuty monitoring of CloudTrail management events is on by default for all accounts that have enabled GuardDuty and is not configurable. CloudTrail S3 data event logs are a configurable data source in GuardDuty. By default, S3 protection is enabled for new detectors, for accounts created before the addition of S3 protection this data source must be enabled manually. The processes for enabling or disabling S3 data event monitoring is covered in this topic.

It is strongly recommended that you enable S3 protection in GuardDuty. If the feature is disabled, GuardDuty is unable to fully monitor or generate findings for suspicious access to data stored in your S3 buckets.

**Kubernetes Protection**

GuardDuty Kubernetes Protection enables Amazon GuardDuty to detect suspicious activities and potential compromises of your Kubernetes clusters within Amazon Elastic Kubernetes Service (Amazon EKS).

Kubernetes Protection is an optional enhancement that enables GuardDuty to consume Kubernetes data sources.

It is recommended that you do not disable Kubernetes Protection in GuardDuty. If the feature is not enabled, the ability of GuardDuty to monitor or generate findings for suspicious activity within your Amazon EKS environment is limited.

**Examples of malwares detected by GuardDuty**

Malware Protection scans for threats such as **trojans, worms, crypto miners, rootkits, and bots**, that might be used to compromise workloads, repurpose resources for malicious use, and gain unauthorized access to data.

**Advantages**

 Accurate, account-level threat detection

 Continuous monitoring across AWS accounts without added cost and complexity

 Threat detections developed and optimized for the cloud

 Threat severity levels for efficient prioritization

 Automate threat response and remediation

**Limitations**

Security findings are retained and made available through the GuardDuty console and APIs for **90 days**. After 90 days, the findings are discarded.