Overview

1. Amazon GuardDuty is a **Threat detection service that continuously monitors** for:
    a. Malicious activity and
    b. Unauthorized behavior to protect your
        i. **AWS accounts,**
        ii. **Workloads**
        iii. **Data stored in Amazon S3**

2. Intelligent Threat discovery to Protect AWS Account

3. It allows you to **monitor for threats** by analyzing:
    a. AWS Cloud Trail Logs,
    b. VPC Flow Logs,
    c. AWS DNS logs.

4. It monitors for:
    a. Instance Compromise
    b. Account Compromise
    c. Bucket Compromise
    d. Reconnaissance activity
    e. Identify exploits on network

5. Uses Machine Learning algorithms, anomaly detection, 3rd party data

6. No need to install any software

7. Input data includes:
    a. **CloudTrail Logs**: unusual API calls, unauthorized deployments
    b. **VPC Flow Logs**: unusual internet traffic, unusual IP addresses
    c. **AWS DNS Logs**: compromised EC2 instances sending encoded data within DNS queries

8. Integration with AWS lambda

9. Amazon Guard Duty maintains 2 types of lists:

Trusted IP list: It consists of IP addresses which are whitelisted and Amazon Guard duty **do not generate** any IP for this list

Threat List : It consists of malicious IP addresses for which Amazon Guard Duty **generates findings**

10. Users from **master accounts** can add or modify the IP addresses from the above list

11. Users from **member accounts** can view the IP addresses from the list

12. Amazon GuardDuty **rules cannot be disabled or deleted** but can be auto archived so any further findings from the rule will not be displayed on Amazon Guard Duty console send to Amazon CloudWatch events for trigger future events

Amazon GuardDuty keeps findings in the Amazon GuardDuty console for **90 days**. After 90 days they are deleted

Go through this: https://aws.amazon.com/guardduty/faqs/

How is Guard Duty different from Amazon Inspector?

1.
Amazon Inspector monitors AWS environment for suspicious activity and generates findings
Amazon Guard duty doesn't generate the suspicious findings.

2.
Amazon Inspector is used for security assessment
Amazon GuardDuty will give your security department the visibility they want into the **identified threats in your AWS environment**