GUARDDUTY EXERCISE AND GUIDED NOTES

REQUIREMENTS: AWS ACCOUNT (not a lab environment)

https://catalog.workshops.aws/guardduty/en-US/introduction

Instructions for an *unfacilitated* workshop.

Complete Modules 1 - 6 own personal AWS account. IMPORTANT: GuardDuty provides a free 30-day trial. To prevent from accruing charges see https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_suspend-disable.html

INSTRUCTIONS:

1. Complete Modules 1 - 6 starting at https://catalog.workshops.aws/guardduty/en-US/module1
2. If you have access to an AWS account, complete the exercises. Note that some steps make reference to a pre-configured lab environment. This is not applicable to this exercise so you may need to edit the instructions based on the resources you have.
3. Answer the guided notes questions below to help with the understanding of concepts and not just mindlessly go through the steps.

Personal Note: The process that works best for me is to complete the lab steps (a little mindlessly, I admit). Read the documentation. Then complete the lab again for better understanding. Use whatever method works best for you.

MODULE 1: AMAZON GUARDDUTY WALKTHROUGH
https://catalog.workshops.aws/guardduty/en-US/module1

1. Amazon GuardDuty offers _____ detection.
2. GuardDuty enables you to continuously monitor and protect AWS accounts, _____ and _____ ins S3.
3. GuardDuty analyzes continuous _____ generated from your account and network activity found in CloudTrail Events, VPC Flow Logs, and DNS logs.
4. GuardDuty uses integrated threat intelligence such as known _____, _____, and ML to identify threats.
5. GuardDuty makes it easy to continuously monitor _____, _____, and data stored in _____.

6. GuardDuty operates **dependently/independently** from other AWS resources so there is no risk of performance or availability impacts to your workloads.
7. GuardDuty is fully _____ with integrated threat intelligence, anomaly detection, and ML.
8. What is a GuardDuty finding?

9. GuardDuty generates a _____ when it detects unexpected and potentially malicious activity in an AWS environment.
10. A _____ allows you to view findings that match the criteria you specify.
11. GuardDuty prices are based on the number of _____ events, _____ audit logs, the volume of _____ and DNS query logs.
12. In the GuardDuty console you can go to _____ in the navigation pane to find average daily costs.
13. Findings are retained and made available in GuardDuty for up to _____ days.
14. You **can/cannot** retain findings longer than 90 days.
15. Enabling _____ to automatically push findings to an S3 bucket can allows you to keep findings for longer than 90 days.
16. S3 protection in GuardDuty is used to monitor _____ to identify potential security risks for data in S3 buckets.
17. GuardDuty monitors threats in S3 resources by analyzing _____ and _____.
18. Kubernetes protection enables GuardDuty to detect _____ and potential compromises of _____ and EKS.
19. Malware Protection in GuardDuty detects suspicious behavior on _____ or _____ workloads.
20. You **can/cannot** manage multiple accounts in GuardDuty.
21. The account you choose to work from is the _____ account for GuardDuty and other accounts are member accounts.
22. What are the two ways you can associate accounts w/ the GuardDuty administrator account?

23. How can you verify if additional protections (S3, Malware, etc) is enabled?

MODULE 2: UNDERSTANDING A GUARDDUTY FINDING
https://catalog.workshops.aws/guardduty/en-US/module2

1. GuardDuty generates a finding when it detects _____ and _____ activity in your AWS environment.
2. Where can you find GuardDuty findings?

3. Describe the security levels for GuardDuty findings.

4. If you want to hide a finding from the Current findings list, what can you do?

MODULE 3: SUPPRESSING FINDINGS
https://catalog.workshops.aws/guardduty/en-US/module3

1. A _____ rule is a set of criteria used to filter finding by automatically archiving new findings based on the criteria.
2. If you choose to use a suppression rule, what is the criteria that need to be set?

3. What is the benefit of using suppression rules?

4. What happens when a finding is generated that matches the suppression rule created?

5. Suppression rules **can/cannot** be created with granular filter criteria.
6. Suppressed findings **are/are not** send to AWS Security Hub, S3, Detective or CloudWatch.
7. You can view suppressed findings in the GuardDuty console by selecting _____ from the findings table.
8. Once suppression rules have been created they **can/cannot** be modified.

MODULE 4: BUILD A THREAT LIST https://catalog.workshops.aws/guardduty/en-US/module4

1. GuardDuty monitors the security of your AWS environment by analyzing and process _____, _____, and _____.
2. You can customize the monitoring scope by configuring GuardDuty to stop alerts for _____ IPs and alert on known _____ IPs from your own threats list.
3. Trusted IP lists and threat lists apply only to traffic destined for _____.
4. The trusted and malicious lists apply to all _____ and _____.
5. The trusted and malicious lists do not apply to _____.
6. GuardDuty **does/does not** generate VPC Flow Log or CloudTrail findings for IP address on trusted IP lists.
7. You can have a maximum of _____ IP addresses and CIDR ranges in a single trusted IP list.
8. You are limited to _____ uploaded trusted IP list per AWS account per Region.

9. Threat lists can be supplied by _____ or created specifically for your organization.
10. GuardDuty generates _____ based on threat lists.
11. You can include a maximum of _____ IP addresses and _____ ranges in a single threat list.
12. GuardDuty generates findings based on activity that involves IP addresses and CIDR ranges in threat lists, findings will not be generated based on _____.
13. You can have up to _____ uploaded threat lists per AWS account per Region.
14. What will happen if the same IP address is on both the trusted and threat IP lists?

15. If managing multiple accounts, how can you apply trusted and threat IP lists to all member accounts?

16. Threat lists only support _____ IP addresses.
17. The S3 _____ can be used as the location of IP lists.
18. IP lists uploaded into GuardDuty **are/are not** automatically activated.

MODULE 5: AGGREGATING FINDINGS WITH SECURITY HUB
https://catalog.workshops.aws/guardduty/en-US/module5

1. AWS Security Hub is a cloud security posture management service that performs _____, _____ best practice checks against your AWS resources.
2. _____ aggregates your security alerts/findings from various AWS services and partner products in a standardized format to allow you to take action on an item.

MODULE 6: SETTING UP GUARDDUTY NOTIFICATIONS

https://catalog.workshops.aws/guardduty/en-US/module6

1. Amazon EventBridge is a _____ that makes it easier to build event-driven applications at scale using events generated from AWS services.

Note: When completing the SNS exercise, check your spam to find the email

Remember, you turn it on - turn it off. See what services you have running and terminate them to prevent an unexpected bill from generating.
https://aws.amazon.com/premiumsupport/knowledge-center/check-for-active-resources/#:~:text=To%20check%20if%20you%20have,AWS%20services%20on%20your%20account.