ENPM665 Homework #4 – AWS GuardDuty Hands On

Version 2.2 – November 15th 2022

Note: This assignment should take approximately 2 hours to complete.

You will be utilizing an exercise that AWS has built. Remember to use **US West 2 (Oregon)** for this exercise.

Start here:
https://github.com/aws-samples/amazon-guardduty-hands-on/blob/master/docs/setup.md
(Ignore steps 1-3, start with 4 – Enabling Guard Duty)

Click the Deploy to AWS image to deploy the CloudFormation stack that will build the items needed for this exercise.

The specific scenarios to complete are:

Scenario 1: Compromised EC2 Instance
https://github.com/aws-samples/amazon-guardduty-hands-on/blob/master/docs/scenario1/index.md

Scenario 2: Compromised IAM Credentials
https://github.com/aws-samples/amazon-guardduty-hands-on/blob/master/docs/scenario2/index.md

Scenario 3: IAM Role Credential Exfiltration
https://github.com/aws-samples/amazon-guardduty-hands-on/blob/master/docs/scenario3/index.md

Once complete follow the clean-up instructions here to remove everything that was create:
https://github.com/aws-samples/amazon-guardduty-hands-on/blob/master/docs/summary.md

Deliverable:

Provide the answers to the questions inside the exercise:

Scenario 1: Compromised EC2 Instance

1. Which data source did GuardDuty use to identify this threat?
2. Will isolating the instance have any effect on an application running on the instance?

3. How could you add more detail to the email notifications?

Scenario 2: Compromised IAM Credentials

1. Which data source did GuardDuty use to identity this threat?
2. What permissions did the user have? (include a screenshot of the user's permissions)
3. Why would the security team decide against setting up an automated remediation?

Scenario 3: IAM Role Credential Exfiltration

1. What are the risks involved with this remediation?
2. What other EC2 instances are using this Role?

Don't forget to do the clean-up at the end of the exercise!