ENPM665 – Cloud Security

Homework – 4

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

UID: 118428369

Email: iamibi@umd.edu

Scenario 1: Compromised EC2 Instance

1. Which data source did GuardDuty use to identify this threat?

A. The data source used by GuardDuty that assist in identifying the threat primarily involved monitored VPC Flow Logs along with CloudTrail and DNS Logs. Additionally, the analysis is performed by considering the custom threat list, machine learning, baselines, etc. to remove unnecessary data and get a clear information of a suspected threat.

2. Will isolating the instance have any effect on an application running on the instance?

A. Depending on whether the application was relying on network-based activity like making GET or POST HTTP calls, the application will start failing on that specific instance. This is because the compromised instance is isolated completely from the network as defined by the rules. If the application had few components that didn't rely on network, they would still be working correctly if the instance is in running condition.

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

A. Using the Input Transformer under Cloud Watch, we can customize the email and add more information like instance id, time of the event, state of the instance, and much more depending on what information the organizations' team feels is sufficient.

Scenario 2: Compromised IAM Credentials

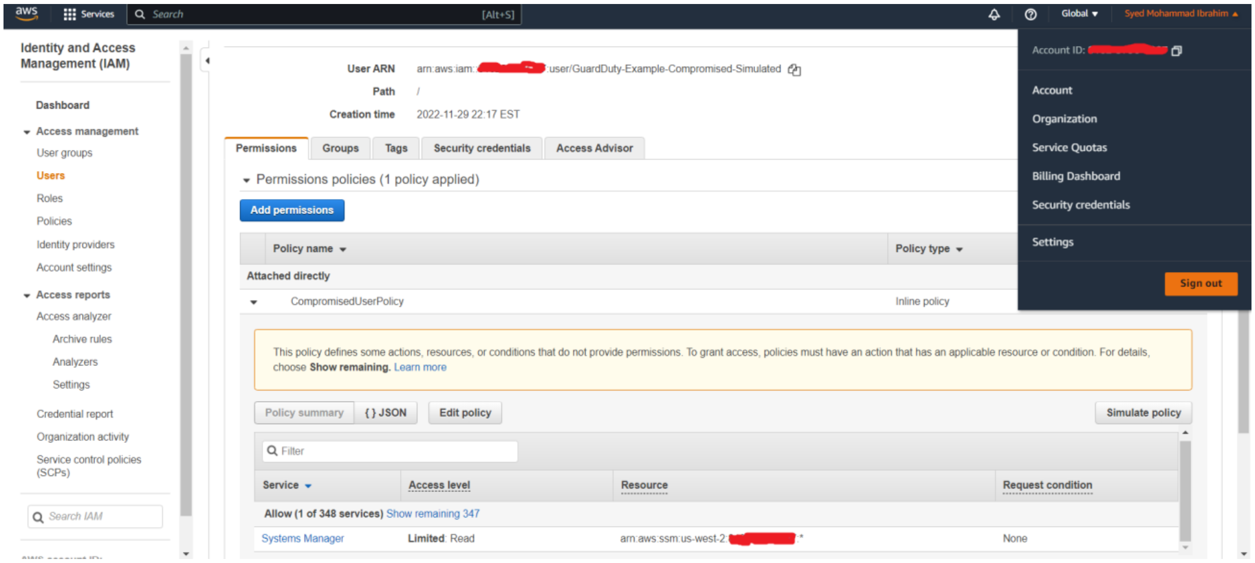
1. Which data source did GuardDuty use to identify this threat?

A. The data source used by GuardDuty that assist in identifying the threat primarily involved monitored Cloud Trail Logs along with VPC Flow Logs and DNS Logs.

Additionally, the analysis is performed by considering the custom threat list, machine learning, baselines, etc. to remove unnecessary data and get a clear information of a suspected threat. The GuardDuty generates findings and sends it to GuardDuty Console and CloudWatch Events.

2. What permissions did the user have? (include a screenshot of the user's permissions)

A. The compromised user had Read permission to the resource as shown in the below screenshot.



User ARN arn:aws:iam::[redacted]:user/GuardDuty-Example-Compromised-Simulated

Path /

Creation time 2022-11-29 22:17 EST

Permissions policies (1 policy applied)

Policy name	Policy type
Attached directly	
CompromisedUserPolicy	Inline policy

This policy defines some actions, resources, or conditions that do not provide permissions. To grant access, policies must have an action that has an applicable resource or condition. For details, choose **Show remaining.** Learn more

Service	Access level	Resource	Request condition
Allow (1 of 348 services) Show remaining 347			
Systems Manager	**Limited**: Read	arn:aws:ssm:us-west-2:[redacted]:*	None

3. Why would the security team decide against setting up an automated remediation?

A. The security team wanted to analyze the compromised users' previous activity to perform an in-depth investigation of such type of incidents. This will provide the team a better scope of the compromise that occurred. This will also tell them whether or not, to report the incident to the specific user or follow standard operating procedures as decided by the security team internally.

Scenario 3: IAM Role Credential Exfiltration

1. What are the risks involved with this remediation?

A. The risks involved with the remediation strategy would be that if there are services that rely on the same role which was revoked, they will be impacted. This will in-turn impact the relevant user(s) which were legitimate. It may also lead to abnormalities in the dependent application functionality.

2. What other EC2 instances are using this Role?

A. The instance using this specific role is “GuardDuty-Example: Compromised Instance: Scenario 3”