Cloud Monitoring

SOP: Setting Up Cloud Monitoring with VPC Flow Logs and AWS Lambda

Objective: Capture network traffic and automate responses to detected threats using VPC Flow Logs and AWS Lambda.

Actionable Steps:

VPC Flow Logs

Enable VPC Flow Logs:

1. Access the VPC Dashboard:
    - Open the AWS Management Console.
    - Navigate to the VPC dashboard.
2. Create Flow Log:
    - Select the VPC you want to monitor.
    - Click on "Actions" and then "Create flow log."
3. Configure Flow Log:
    - Filter: Choose the type of traffic to capture (All, Accept, or Reject).
    - Destination: Select the destination for the flow logs (CloudWatch Logs or S3).
        - CloudWatch Logs:
            - Choose "Send to CloudWatch Logs."
            - Specify or create a new log group.
        - S3:
            - Choose "Send to an S3 bucket."
            - Specify the S3 bucket where logs will be stored.
4. Review and Create:
    - Review the configuration.
    - Click on "Create flow log."

Create Log Groups and Streams:

1. Organize Flow Logs:
    - If using CloudWatch Logs, ensure that log groups and streams are organized logically.
    - Create log groups for different VPCs or traffic types to simplify management and analysis.

AWS Lambda

Create a Lambda Function:

1. Access the Lambda Dashboard:
   - Open the AWS Management Console.
   - Navigate to the Lambda dashboard.
2. Create Function:
   - Click on "Create function."
   - Choose "Author from scratch."
   - Enter a name for the function.
   - Choose a runtime (e.g., Python, Node.js).
   - Configure the execution role (create a new role with basic Lambda permissions).

Configure the Lambda Function to Respond to VPC Flow Logs:

1. Write Lambda Function Code:
   - Write the code to process VPC Flow Logs and trigger appropriate actions. Example code (Python):

python

[redacted]

```
import json import boto3 def lambda_handler(event, context): # Process the VPC Flow Log
event log_data = json.loads(event['Records'][0]['body']) # Example action: print log data
print(log_data) # Example action: trigger an alert or another AWS service # (e.g., send a
notification, block an IP, etc.) return { 'statusCode': 200, 'body': json.dumps('Log processed
successfully') }
```

2. Set Up Triggers for the Lambda Function:
   - In the Lambda function configuration, add a trigger.
   - Select the appropriate log source (e.g., CloudWatch Logs).
   - Configure the trigger to invoke the Lambda function based on specific log events or patterns.

Test and Deploy the Lambda Function:

1. Test with Sample Log Data:
    - Create a test event in the Lambda console using sample log data.
    - Run the test and verify the function's output and actions.
2. Deploy the Lambda Function:
    - After successful testing, deploy the Lambda function.
    - Monitor the function's execution and performance.

Verification and Monitoring:

1. Monitor CloudWatch Logs and Lambda Execution:
    - Regularly check CloudWatch Logs for VPC Flow Log entries.
    - Monitor the Lambda function's execution logs and performance metrics in the AWS Lambda console.
2. Set Up Alerts and Notifications:
    - Configure CloudWatch Alarms to alert you of specific log events or Lambda execution issues.
    - Set up SNS (Simple Notification Service) for email or SMS notifications.

Training and Documentation:

1. Provide Training:
    - Train the team on how to use CloudWatch Logs, Lambda, and monitoring tools effectively.
    - Ensure everyone understands how to interpret log data and respond to alerts.
2. Document Configuration and Procedures:
    - Maintain documentation for the VPC Flow Log and Lambda function configuration.
    - Include details on how to modify and update the Lambda function code as needed.