SIEM/Log Aggregation System

SOP: Setting Up a Log Aggregation System with AWS CloudTrail and CloudWatch

Objective: Capture network traffic and automate responses to detected threats using AWS CloudTrail and CloudWatch

Actionable Steps:

CloudTrail

Enable CloudTrail:

1. Access the CloudTrail Dashboard:
   - Open the AWS Management Console.
   - Navigate to the CloudTrail dashboard.
2. Create a trail:
   - Under Trails, click on “Create trail.
3. Configure the trail:
   - Choose a trail name for the new trail.
   - Create a new S3 bucket or specify an existing S3 bucket.
     - If creating a new bucket, choose a name or use the default name provided.
     - If creating a new bucket create an AWS KMS alias
   - Navigate CloudWatch logs
     - Enable CloudWatch Logs
     - Choose a new log group name or use the default log group name
     - Under “IAM Role”, select “New”
     - Choose a Role name
   - Select “Next” at the very bottom
   - In “Choose log events”, choose which event types to log
     - Management event for logging management operations
     - Data events for logging resource operations
     - Insights events for logging unusual activity, errors, or user behavior
   - Select “Next” at the very bottom
4. Review and Create:
   - Review the configuration.
   - Click on "Create flow log."
5. Access the CloudWatch dashboard
   - Open the AWS Management Console
   - Navigate to the CloudWatch Dashboard
6. Create a metric filter

   - Select the CloudTrail log group
   - Select metric filters below
   - Click create a metric filter
   - Enter a filter pattern to specify a pattern
   - Select “Next” on the very bottom
   - Assign the metric
     - Enter a filter name
     - Create or specify a metric namespace
     - Enter a metric name
     - Enter a metric value
   - Select “Next at the very bottom”
7. Review and Create:
   - Review the configuration.
   - Click on "Create metric filter."
8. Create an alarm
   - Select the metric you want to be alerted for
   - Click “Create alarm”
   - Specify metric and conditions
     - Select threshold type
     - Define the alarm condition
     - Define a threshold value
   - Configure actions
     - Select an alarm state trigger
     - Define the SNS topic that will receive notification
       - If selecting an existing SNS topic, select an SNS topic
       - If creating a new topic, create a topic name and type email endpoint(s)
       - If using topic ARN, enter a topic/ARN
   - Name and description
     - Create an alarm name
9. Review and create
   - Review the configuration
   - Click on “Create alarm”

CloudWatch

Analyze CloudWatch Logs:

1. Analyzing CloudWatch Logs Insights:

- Select “Logs Insights”
- Select the log group to query
- Click on “Run query” to see events of the log group

Verification and Monitoring:

1. Monitor CloudWatch Logs and Lambda Execution:
    - Regularly check CloudWatch Logs from EC2 and VPC events.
2. Set Up Alerts and Notifications:
    - Configure CloudWatch Alarms to alert you of specific log events
    - Set up SNS (Simple Notification Service) for email or SMS notifications.

Training and Documentation:

1. Provide Training:
    - Train the team on how to use CloudTrail, and CloudWatch effectively.
    - Ensure everyone understands how to interpret log data and respond to alerts.
2. Document Configuration and Procedures:
    - Maintain documentation for CloudTrail creation and CloudWatch logging