AWS Cloud Risk Assessment

User Instructions for MacOS/Linux

Prerequisites:

1. An organization CloudTrail trail that logs activity events. Read more on how to create a trail for an organization.
2. An Amazon S3 bucket receiving trail log files.
    a. AWS S3 console access
    b. The risk assessment will analyze the log events stored on the corresponding S3 bucket. Read more about log retention defaults.
    c. To check the retention period you can use: aws s3api get-bucket-lifecycle-configuration --bucket [bucket-name]
3. An AWS user with read permissions to access the content of the S3 bucket where the CloudTrail logs are stored.
    a. Aws-risk-assessment uses the same authentication methods as the AWS CLI to access your AWS resources and their services. The policies that grant permissions are the same because the AWS CLI calls the same API operations that are used by the service console. Read more about Installing AWS CLI.
    b. To grant read permissions to your user we recommend using a group/role with the ReadOnlyAccess policy attached. Read more about Policy Management for IAM users
4. The risk assessment binary executable provided. If you do not have the file, please go to https://sysdig.com/campaigns/aws-cloud-risk-assessment/ where you can download it.

Instructions:

1. Unzip the file by right clicking and extracting the content.
2. Open Terminal (MacOS/Linux)
3. Cd to the folder where the extracted files are located: cd /path/of/folder
4. Give execute permissions to the binary chmod +x aws-risk-assessment

    Note for MacOS users: If your device has an AMD processor (Intel) then execute the **aws-risk-assessment-darwin-amd64** binary. For ARM (Apple M1) processor, please use the **aws-risk-assessment-darwin-arm64**

5. Run the tool a first time as ./aws-risk-assessment --help to understand the parameters required. i.e. the S3 bucket name where the CloudTrail logs are stored and the region of the bucket. You can find this information in the S3 Console of your AWS account.
6. Indicate the details using the command ./aws-risk-assessment --bucket [your-cloudtrail-s3] --region [region-s3]

7. Launch the binary.
8. Depending on the number of users, activity and cloud infrastructure size, the assessment will complete and a PDF report will be generated within the same folder as the binary.
9. Review the AWS Cloud Risk Assessment Report to see any potential threats identified.

If you need any help with the report or the assessment please get in touch with us and we will be happy to help!