NG SIEM - AWS Integration

Overview

The AWS Integration enables the collection of logs and metrics from your Amazon Web Services (AWS) environment. This integration helps centralize security and operational data for monitoring, investigation, and reporting.

Data Streams

The AWS integration collects two main types of data:

1. **Logs** – Records of events that occur within your AWS account.
   Examples:
   - Every request received by CloudFront
   - Actions performed by AWS users or roles
   - API activity captured by CloudTrail
2. **Metrics** – Real-time insights into the performance and health of AWS services.
   Examples:
   - CPU utilization of EC2 instances
   - S3 storage usage
   - RDS performance metrics
   - AWS cost and usage breakdowns

Requirements

Before configuring the AWS integration, ensure you have:

1. **AWS Credentials** – To connect to your AWS account.
2. **AWS Permissions** – To grant access to the necessary AWS services.

Step 1. Create IAM User and Custom Policy

1. **IAM User**
   -an identity you create in **AWS Identity and Access Management (IAM)** that represents a person or application which needs to interact with your AWS resources.
2. **User Policy and Permissions**

The IAM User must be granted the following permissions:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ce:GetCostAndUsage",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "iam:ListAccountAliases",
        "inspector2:ListFindings",
        "logs:DescribeLogGroups",
        "logs:FilterLogEvents",
        "organizations:ListAccounts",
        "rds:DescribeDBInstances",
        "rds:ListTagsForResource",
        "s3:GetBucketLocation",
        "s3:GetObject",
        "s3:ListBucket",
        "sns:ListTopics",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues",
        "sqs:ReceiveMessage",
        "sts:AssumeRole",
        "sts:GetCallerIdentity",
        "tag:GetResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Step 2: Create Access Key

Long-term credentials associated with an IAM user or the AWS root account.

- 1. **Access Key ID** – First part of the access key
  2. **Secret Access Key** – Second part of the access key

Step 3: Create a CloudTrail Trail and Send Logs to S3

Set up an AWS CloudTrail trail to record account activity and deliver log files into an S3 bucket for secure storage, auditing, and compliance monitoring.

1. **Open CloudTrail** > Create a **New Trail**
2. **Trail Settings**
   - Trail name: Enter a unique name.
   - Apply trail to all accounts in my organization.
3. Choose an S3 Bucket
   - **Storage location** → Select **Create new S3 bucket** or **Use existing bucket**.

   If using **new bucket**:
   - Enter a bucket name.
   - CloudTrail will create the bucket and add the correct permissions.

   If using **existing bucket**:
   - Select your bucket from the dropdown.
   - CloudTrail will prompt you to allow access. Click **Yes** to let CloudTrail update the bucket policy.
4. Additional Settings
   - **Enable for all accounts in my organization**
   - **Log file SSE-KMS encryption:** Enable if you want encryption with a KMS key(optional).
   - **Log file validation:** Enable to verify log integrity.
5. Choose Log Events
   1. **Event Type**
      - **Management events** - Capture management operations performed on your AWS resources.
      - **Data events** - Log the resource operations performed on or within a resource.
      - **Insights events** - Identify unusual activity, errors, or user behavior in your account.
      - **Network activity events** - Network activity events provide information about resource operations performed on a resource within a virtual private cloud endpoint.
   2. **Management events:**
      - Check **Read**(default is usually All).
6. Review and Create
   - Review your configuration summary.
   - Click **Create trail**.

To configure the AWS Integration:

> **Please provide the following information to CyTech Support:**

- **Access key ID**
- **Secret Access Key**
- **Region**
- **Trail Log Collection > S3 Bucket ARN**

*If you need further assistance, kindly contact **support@cytechint.com** for prompt assistance and guidance.*

Revision #4
Created 23 September 2025 08:03:06 by Richmond Abella
Updated 3 October 2025 12:39:05 by Richmond Abella