NG SIEM- AWS CSPM Integration

Introduction

CSPM discovers and evaluates the services in your cloud environment, like storage, compute, IAM, and more, against hardening guidelines defined by the Center for Internet Security (CIS) to help you identify and remediate configurations risks like:

- Publicly exposed storage buckets
- IAM Users without MFA enabled
- Networking objects that allow ingress to remote server administration ports (22, 3389, etc.)

Recommendation

Set up cloud account access

The CSPM integration requires access to AWS's built-in `SecurityAudit` IAM policy in order to discover and evaluate resources in your cloud account. To provide access we need:

- **IAM Role**
- **Direct access keys**

Create IAM User

Follow AWS's IAM roles for Amazon EC2 documentation to create an IAM role using the IAM console, which automatically generates an instance profile.

1. Create an IAM role:
    1. In AWS, go to your IAM dashboard. Click **Roles**, then **Create role**.
    2. On the **Select trusted entity** page, under **Trusted entity type**, select **AWS service**.
    3. Under **Use case**, select **EC2**. Click **Next**.
    4. On the **Add permissions** page, search for and select `SecurityAudit`. Click **Next**.
    5. On the **Name, review, and create** page, name your role, then click **Create role**.

2. Attach your new IAM role to an EC2 instance:

1. In AWS, select an EC2 instance.
2. Select **Actions > Security > Modify IAM role**.
3. On the **Modify IAM role** page, search for and select your new IAM role.
4. Click **Update IAM role**.

3. **Create Direct access keys**
   Access keys are long-term credentials for an IAM user or AWS account root user. To use access keys as credentials, you must provide the `Access key ID` and the `Secret Access Key`. After you provide credentials, finish manual setup.

   For more details, refer to Access Keys and Secret Access Keys.

   - `Access key ID`: The first part of the access key.
   - `Secret Access Key`: The second part of the access key.

> Please provide the following information to CyTech:

- **Access Key ID**
- **Secret Access Key**

Revision #4
Created 23 September 2025 08:04:13 by Richmond Abella
Updated 18 November 2025 10:23:16