Hi All,

Good Morning & Good Evening!

Today I'm going to talk about the IAM Roles Audit. This presentation would be predominantly on the issues that we found during the audit and plan of action to streamline those issues.

This is the agenda of the presentation:

Let's discuss about the IAM Role and its importance. IAM roles are IAM identities that can be created with set of permissions policies to achieve the task. The difference between IAM User and Role is, User may have access keys that are long term credential and wouldn't be changed until and unless we rotate them, but where in roles generates temporary credentials for the session that we establish. Apart from this, roles can be used by anyone who needs it to accomplish the task. But, access keys would stick single user for long time. Since everyone can use roles, need to check the necessity of their existence and permissions that were provisioned. So, we decided to audit the IAM roles to cleanup across all the accounts.

To collect the role information, we used same infra that we are using for access keys. This is the infra, where we are switching to accounts and gathering the roles information.  The report looks like this: It has Role name, RoleId, Role ARN, Creation date, Last used date, Policy names that were attached to role, Trust Relationship, Policy Documents and Account Number.  Out of all these, we mainly looking at creation date, last used date to calculate the role age and last usage. Trust relationship and Policy documents are used to review the permissions that each role has.

We have categorised the roles into Four types:

1. Core roles
2. Service roles
3. Security roles
4. Application roles

Roles with Okta integration with AD are considered as **Core Roles**. For core roles, the trust relation would like this.

**Service Roles** are mainly used by applications and there were tagged as "Function = Service-Role".

**Security Roles** are used by security applications and teams and these have root level permissions under the trust relationship.

**Application Roles** has permissions to specific AWS services and these are mainly used by application teams.

Based on these categories, we did analysis on these roles and this is the Roles Audit Summary:

1. We have identified many roles those were created manually using AWS cli and console and we come to know that few teams are using their own terraform scripts for the accounts that they handling.
2. Nearly ~4.6k roles were created and unused since after the creation
3. Many roles were overly permissive with permissions
4. Core and service roles were heavily modified across many accounts

To resolve all these issues, we have immediate goals and plan of actions on these:

1. Roles that created and not used for more than 90 days will be reviewed and considered for the deletion.
2. Overly permissive permissions will be cut down with minimal/required permissions.
3. Operations on roles must be happened at TF level that are maintained by SRE team
4. Tag policies would be enforced on roles as per the categorisation.
5. We are going monitor role usage with event tackers such as Guardrail and cloudtrail.
6. Correlate roles with TF for better management and SCPs would be deployed at OU level to restrict the role modifications.