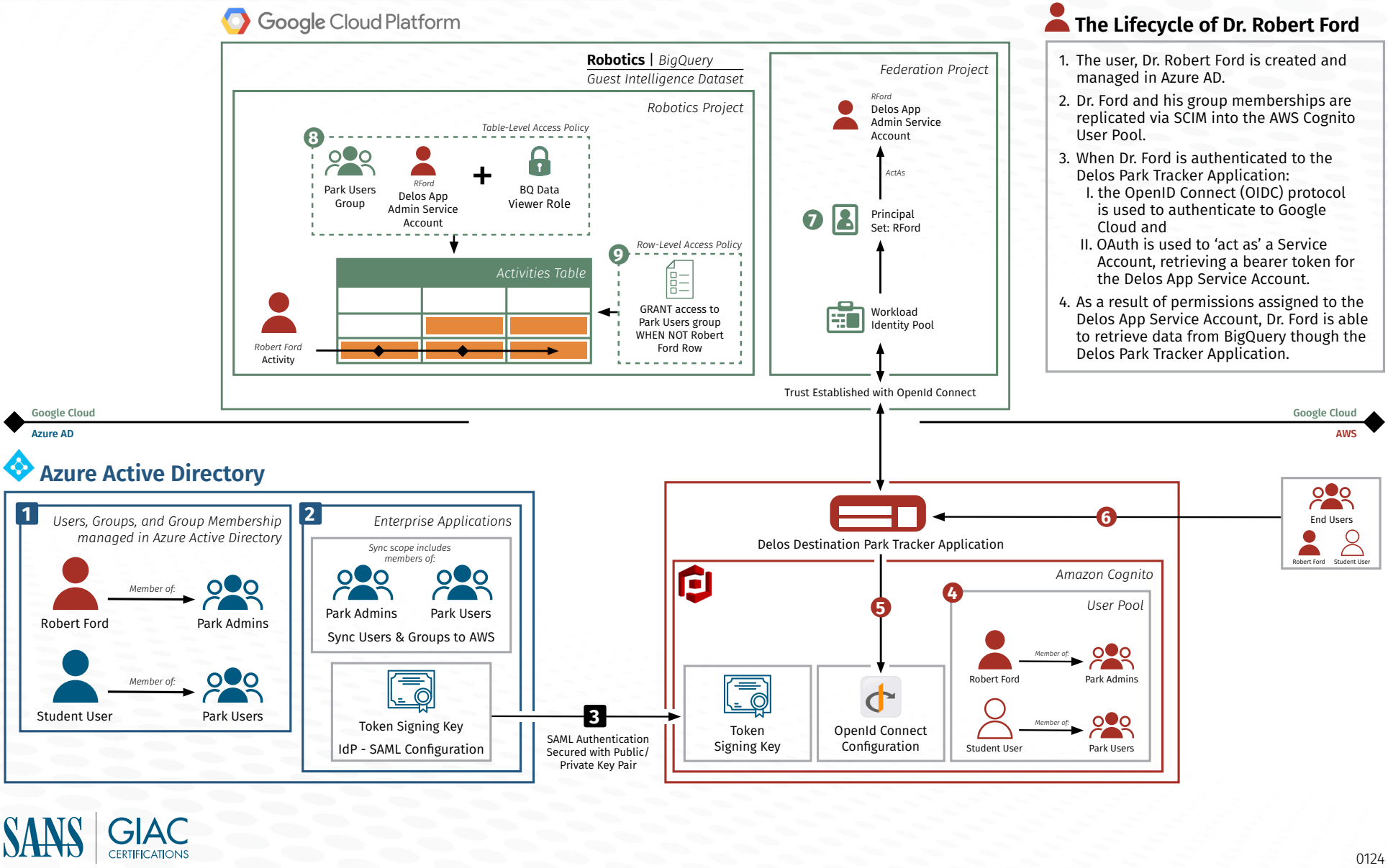
BigQuery Access Architecture

CLOUD SECURITY

Created by Kat Traxler and Eric Johnson, co-authors of
SEC549: Enterprise Cloud Security Architecture | *sans.org/sec549*



The Lifecycle of Dr. Robert Ford

1. The user, Dr. Robert Ford is created and managed in Azure AD.
2. Dr. Ford and his group memberships are replicated via SCIM into the AWS Cognito User Pool.
3. When Dr. Ford is authenticated to the Delos Park Tracker Application:
   I. the OpenID Connect (OIDC) protocol is used to authenticate to Google Cloud and
   II. OAuth is used to 'act as' a Service Account, retrieving a bearer token for the Delos App Service Account.
4. As a result of permissions assigned to the Delos App Service Account, Dr. Ford is able to retrieve data from BigQuery though the Delos Park Tracker Application.

SANS | GIAC CERTIFICATIONS

BigQuery Access Architecture

DIAGRAM KEY

1. User and groups managed within Identity Provider (Azure AD).
2. Azure Enterpeise Applications used to sync in-scope users and groups to AWS Cognito User Pool and configure SAML federation.
3. SAML tokens signed and secured with private key stored in Azure AD, public key exported to AWS Cognito User Pool configuration and used to validate SAML tokens.
4. In-scope users and groups are replicated to the AWS Cognito User Pool directory.
5. Cognito OpenID Connect (OIDC) trust established between Delos Destinations Park Tracker App, hosted in AWS, and the Google Cloud Federation project.
6. End Users, both Park Admin and Park User groups, access the Park Tracker Application to retrieve Guest Intelligence data from the BigQuery dataset in the Google Cloud Robotics project.
7. The Google Cloud Federation project's Workload Identity Pool is configured to allow only the principal Dr. Robert Ford to impersonate the Delos App Admin Service Account.
8. End Users, both Park Admin and Park User groups, have the BigQuery Data Viewer role allowing access to the Guest Intelligence BigQuery dataset. These members can sign into the Google Cloud web console and query the 'Activities' BigQuery table.
9. BigQuery Row-Level Access Policy applied to the 'Activities' table blocks the Park Users group from directly accessing rows containing Dr. Robert Ford's data. This policy forces row-level access to Dr. Robert Ford's data to use the Delos App Admin Service Account. Dr. Robert Ford must authenticate to the Park Tracker Application, exchange the Cognito identity token with a Google Workload Identity Pool token, and impersonate the Delos App Admin Service Account to view the restricted 'Activities' data.