Customer Story: Establishing Secure GCP Lifecycle Pipeline

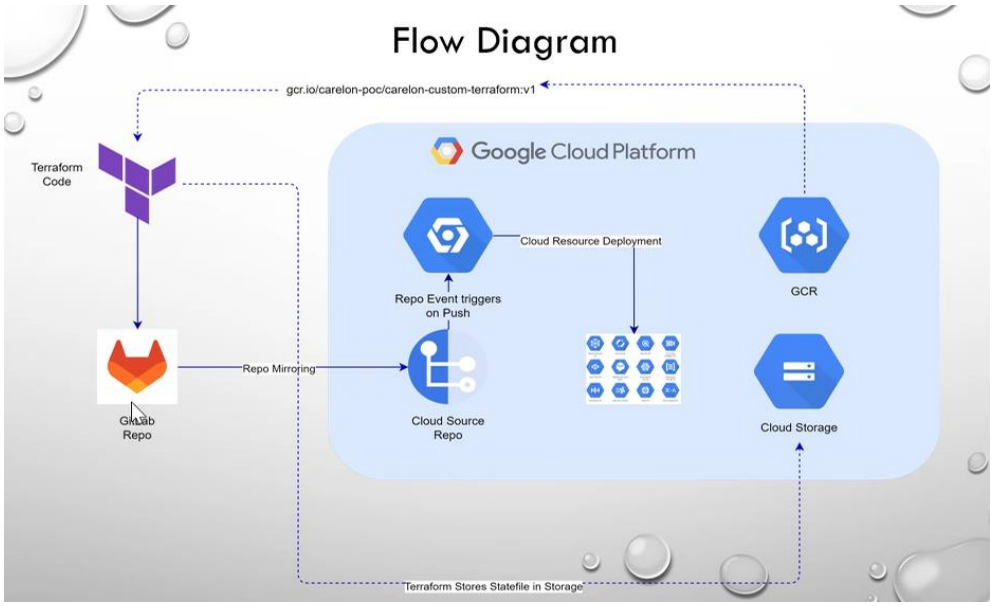
When a digital healthcare company, focused on value-driven outcome and connected care experiences, began their digital transformation into GCP, they sought the expertise of Edge Consulting. The initial milestone objective was for the IT team to establish a new greenfield GCP Landing Zone (LZ) with baselevel security controls within 30 days.

Edge began the engagement by establishing the foundational Organization Policies. Then, Edge created the service account associated with the new GCP LZ. To lock down the service account, Edge applied security policies to the service account. Some of the most important security policies we applied to secure service account creation and use included:

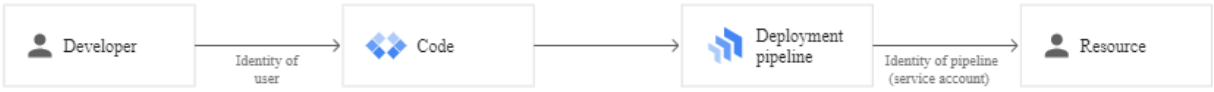
1. Disable service account creation in Organization Policies - so only approved security personnel can create service accounts;
2. Disable service account key creation - to prevent service accounts from being leaked or compromised; and
3. Disable source code download – to keep source code secured and prevent source code exfiltration.

Edge was also asked to securely integrate to the customer's GitLab environment. This was a challenge since ***GCP Cloud Source*** Repositories does not natively provide automated integration with GitLab. The customer was very keen on getting visibility into what the developers were doing within their Gitlab environment. Overall, the customer wanted to protect source code, track development activities, and require application developers to follow the established secure code promotion process. This required Edge to get creative.

For the solution**,** Edge coded the needed script to connect GitLab and Cloud Source. Then Edge leveraged **Google Cloud Build** and **Google Container Registry (GCR)**, custom Docker image, and Terraform code to build out a deployment pipeline. The diagram below depicts the overall deployment lifecycle architecture Edge created.



Attention to security details was needed to ensure the service account met the company's service account security standards. Locking the service account down so that it could only be used for its intended purpose while eliminating the possibility of a human hijacking the service account was of primary importance to the customer. One of the security precautions taken by Edge was to ensure the service account was registered in the customer's CyberArk vault. One of the other security precautions was to configure and associate the service account with a deployment pipeline role. This ensures only the service account identity is used to execute the pipeline deployment.



Requiring a deployment pipeline use a service account to access the customers GCP LZ has the following advantages:

- By configuring a pipeline to use a service account, you ensure that code can be deployed even if the author of the code is no longer with your organization.
- This approach can make it easier to manage IAM policies and allows for requiring users consistently use the deployment pipeline to perform all modifications.

The customer admitted their timeline was aggressive, but the visibility and tracking of application development activities is essential for meeting the company's security and audit controls. In the end, the customer appreciated the work Edge delivered, especially given the very limited in-house GCP security expertise available for this high-priority endeavor. Moving at the speed of business is always a challenge, and we appreciate Edge for being an important extension of our Cloud security team.