Some security improvements I have noticed that should be fixed in order to protect the clusters from outside/internal malicious attacks.

1. Gcr-json-key.yaml in the **nymcard-platform-infra-azure-dev** contains unselead secrets like **gcr-json-key.yaml** from where it can be extracted a gcp service-account with read/write access to the nymcard-platform gcp project docker registry.

2. "packer-sa@nymcard-common-services.iam.gserviceaccount.com" gcp SA on nymcard-platform-common-services has Editor access to the project.

3. gs://nymcard-terraform-state/inc-neo-gb-1-stg-infra/terraform/rke/default.tfstate contains unprotected secrets like the admin-vm tls-private key and the kubernetes config, this applies to all the TF state files containing sensitive informations.

4. Able to SSH into the admin-vms outside the VPN ips with only the ssh key, this should not be permitted and only allowed through the VPN.

5. SSH to any public host shouldn't be allowed from inside admin-vm or the Kubernetes Nodes; this would protect the nodes from the doing reverse SSH to external IP(s).

6. Each Kubernetes Fluxcd enabled cluster should only be allowed to clone the Environment project and no other projects (ex. You can clone and write to all the Bitbucket projects from inside a Fluxcd pod with access to the bitbucket).

7. Kubernetes clusters should only accept only signed docker images that are signed at the build time and verified inside the cluster (ex. https://github.com/sigstore/cosign) this would protect the cluster from *malicious docker images* (ex: image containing reverse ssh tunnels or malicious code).

8. Default service account token with access to all Kubernetes API is automatically mounted into a new pod if no specific service account is specified, this gives access to the Kubernetes API from all the pods. “automountServiceAccountToken: false”

9. Disable anonymous access to the Kubernetes API

10. Disable Privileged containers deployment,through PodSecurityPolicy or RKE settings;

11. Denying container features, such as hostPID, hostIPC, hostNetwork, allowedHostPath

12. Rejecting containers that execute as the root user or allow elevation to root.

13. LimitRange and ResourceQuota are two policies that can limit resource usage for namespaces or nodes.

14. K8s API insecure port 8080 should be disabled; can be disabled using the API server flag --insecure-port=0.

15. Inside the Cluster all the secrets can be accessed because they don't have any encryption; , secrets can be encrypted by configuring data-at-rest encryption on the API server or by using an external Key Management Service (KMS), which may be available through a cloud provider. To enable Secret data-at-rest encryption using the API server, administrators should change the kube-apiserver manifest file to execute using the --encryption-provider-config argument.

    Recommended tools:

    - https://falco.org/
    - https://github.com/sigstore/cosign/releases
    - https://sysdig.com/
    - https://istio.io/ / https://linkerd.io/