**Product Management Trainee Assignment – Problem Statement 2**

**1. Overview**

This task involves setting up a local Kubernetes (K8s) cluster and scanning it using a security tool to identify vulnerabilities or misconfigurations. Tools like Kubescape are used to perform these scans. The final result will be a JSON file that lists all the findings from the security scan.

**2. Steps Taken**

1. Set up a Local Kubernetes Cluster

- Installed Minikube as the local Kubernetes environment.  
- Verified cluster is up and running using 'kubectl cluster-info'.

2. Installed Kubescape

- Downloaded and installed Kubescape from the official GitHub repository.  
- Confirmed the installation using 'kubescape version'.

3. Performed Security Scan

- Ran the scan on the active Minikube cluster using the command:  
 kubescape scan framework nsa --output json --output-file results.json  
- This command scanned the cluster using the NSA benchmark framework and saved results in JSON format.

**3. Output Details**

The JSON file contains detailed information about:

- Cluster configurations

- Failed controls and severity

- Namespaces and resource details

- Suggestions for remediation

**4. Conclusion**

The Kubernetes cluster was successfully scanned using Kubescape. The scan report in JSON format provides important findings that help secure the cluster by identifying weak configurations and potential risks. The findings are ready to be shared as part of this submission.