Mary Mitchell (mem0250)
COMP5710-001
Due Date: September 19, 2022
Workshop 3: Resilient Automated Configuration Management

Three Most Frequent Security Misconfigurations:

1. NO_NETWORK_POLICY: The misconfiguration category that is related with not specifying network policies. Without specifying network policies Kubernetes installations are susceptible to unauthorized accesses.

2. INSECURE_HTTP: The category of using HTTP without SSL/TLS certificates to setup URLs or transmit traffic inside and outside the Kubernetes clusters. Without SSL/TLS certificates, the data transmitted across Kubernetes objects are susceptible to main-in-the-middle (MITM) attacks.

3. NO_ROLLING_UPDATE: The misconfiguration category that is related with not explicitly specifying RollingUpdate in the configuration file. A lack of rolling updates makes a Kubernetes installation susceptible to supply chain related attacks.