**COMP-5710 Workshop 2:**

**Resilient Automated Configuration Management**

**User: Will May (wdm0032@auburn.edu)**

**Most frequent security misconfigurations detected:**

1. NO\_NETWORK\_POLICY [46]
2. INSECURE\_HTTP [25]
3. NO\_ROLLING\_UPDATE [24]

**Description:**

1. NO\_NETWORK\_POLICY:
   1. 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
   1. 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
   1. 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.