#### **Seminar 1: STRIDE and DREAD tools**

Top three vulnerabilities:

1. Network Security Solutions
2. Network Protocols
3. Unsecure Software

Dread Analysis

1. 3-High Risk
2. 2-Medium Risk
3. 2-Medium Risk

Threat Mitigation Ranked Highest to Lowest.

1. Zero Trust Architecture
2. IPS/IDS
3. Packet Filtering
4. Honeypot
5. Account Lockout
6. Cyber Training
7. Two Factor Authentication

The risk with the highest rating was given to vulnerable network security solutions. The network is arguably the most crucial part of a business to secure. An unsecured one can allow for numerous cyber attacks. Other vulnerabilities that follow it are insecure network protocols and insecure software. To mitigate them severe solutions could be proposed such as zero trust architecture, which would force everyone to authentication. As well an IPS could be implemented to perform packet inspection, which could potentially stop an attack. However, these solutions assume several things about a network that are unknown. Given that there is numerous amount of network solution, protocols, and software. It makes it difficult to propose a catch-all solution.