**Describe MITRE ATT&CK FRAMEWORK and how it applies to threat detection**

The MITRE ATT&CK Framework is a framework that documents known cyber threats and adversaries and displays the tactics, techniques, and procedures that they use. The TTPs that threats utilize can be compared and contrasted using the MITRE ATT&CK Navigator tool. The MITRE ATT&CK Framework applies to threat detection because it can be used as a tool to find known malware and threat actors that target specific sectors like medicine and finance.

**Pick 3 TTPs to discuss and explain**

Initial Access | Replication Through Removable Media - ID: T1091. Malware is copied onto removable media such as a USB drive which is then connected to the target system. When connected to the system Autorun features are used to execute any malicious software on the drive.

Defense Evasion | Indicator Removal - ID: T1070. The deletion or modification of pieces evidence of an attackers presence in a system. These pieces of evidence can inclue log files, events, etc.

Exfiltration | Exfiltration Over C2 Channel - ID:T1041. Exfiltration of stolen data over a pre-existing command and control channel. Data is transferred to a command and control server.

**How are IoCs used in Threat Hunting**

Indicators of compromise are any signs that a system may have been attacked or compromised. Indicators of compromise are used in Threat Hunting by being a starting point to look for possible threats. An IoC such as network traffic anomalies can be used to show signs of malicious activity in the network such as data exfiltration.