Tactics Group	Tactic Question	Supported? (Y/N)	Risk	Design Decisions & Location	Rationale & Assumptions
Detecting Attacks	Does the system support the **detection of intrusions** by, for example, comparing network traffic or service request patterns within a system to a set of signatures or known patterns of malicious behavior stored in a database?				
	Does the system support the **detection of denial-of-service attacks** by, for example, comparing the pattern or signature of network traffic coming into a system to historical profiles of known DoS attacks?				
	Does the system support the **verification of message integrity** via techniques such as checksums or hash values?				
	Does the system support the **detection of message delays** by, for example, checking the time that it takes to deliver a message?				
Resisting Attack	Does the system support the identification of actors through user IDs, access codes, IP addresses, protocols, port, etc.?				
	Does the system support the authentication of actors via, for example, passwords, digital certificates, 2FA, or biometrics?				
	Does the system support the authorization of actors, ensuring, that an authenticated actor has the right access and modify either data or services?				
	Does the system support limiting access to computer resources via restricting the number of access points to the resources, or restricting the thype of traffic that can go through the access points?				
	Does the system support limiting exposure by reducing the amount of data or services that can be accessed through a single access point?				
	Does the system support data encryption, for data in transit or data at rest?				
	Does the system design consider the separation of entitites via physical separation on different servers attached to different networks, virtual machines, or an "air gap"?				
	Does the system support changing credential settings, forcing the user to change those settings periodically or at critical events?				
	Does the system validate input in a consistent, system-wide way-for example, using a security framework or validation class to perform actions such as filtering, canonicalization, and sanitization of external input?				