GenCyber Concepts

Objectives

- Learn the basic, cross-cutting concepts of cybersecurity
- Discuss GenCyber concepts

GenCyber Concepts

The following are the six GenCyber concepts (**CIATDK**):

- Confidentiality
- Integrity
- Availability
- Think like an adversary
- Defense in depth
- Keep it simple

The first three of the GenCyber concepts are called the CIA triad. They are confidentiality, integrity, and availability.

Confidentiality

Confidentiality means the data is hidden, unreadable, or otherwise secret to unauthorized parties.

Examples are

- Encrypted files and network traffic

- Classification systems
- Locked safe

Integrity

Integrity means the data can be proven to be unchanged by unauthorized parties.

Examples are

- Hashing
- Secure logs
- Email signatures

Availability

Availability means data should be reasonably available when it needs to be.

Examples are

- Preprocessing
- Load balancing
- Security-functionality tradeoff

Think Like an Adversary

Thinking like an adversary means to consider the potential actions of the opposing force (adversary) working against the desired result. This means being able to anticipate the actions of your adversary and building security measures to defend your information.

Defense in Depth

Defense in depth means having multiple layers of security controls in place. If one layer fails, another layer is in place to stop the attack.

Keep It Simple

Keep computer programming and system design simple without compromising the ability to protect information from unauthorized access.

Time to Dig Deeper

Think of a representation of your assigned concept. Have a team member draw it. You will have 10 minutes.

Once you finish, present the drawing to the class.