Student: Maciej Mateusz Madejsza
ID: MAD21541198
Module: SSD

Security Requirements

Defence Ventures

1. Multi-Factor Authentication (MFA) for User Access

- **Asset**: User accounts.
- **Threat**: Spoofing.
- **Narrative**: Attackers may pose as users in order to obtain unapproved access.
- **Work Required**: All user logins should have multi-factor authentication (MFA), with sensitive operations needing a second factor.
- **Verification**: Check for MFA enforcement and confirm password-only access prohibition.

2. Data Encryption in Transit and at Rest

- **Asset**: Sensitive data.
- **Threat**: Information Disclosure.
- **Narrative**: Data that isn't encrypted can be intercepted.
- **Work Required**: Encrypt data with AES-256 at rest and TLS in transit, secure key management.
- **Verification**: Verify transmission security using packet inspection and confirm encryption in code reviews.

3. Logging and Audit Trails for Sensitive Actions

- **Asset**: System logs.
- **Threat**: Repudiation.
- **Narrative**: Malicious users might erase logs to hide illegal activity.
- **Work Required**: Keep an eye out for tampering and record any sensitive acts with limited access.
- **Verification**: Use packet inspection to verify transmission security, and use code reviews to validate encryption.

AstroDev

1. Role-Based Access Control (RBAC) for Mission Data

- **Asset**: Mission data and adjustment settings.
- **Threat**: Tampering.
- **Narrative**: Unauthorized access to mission data may result in detrimental modifications that impact spacecraft functionality.
- **Work Required**: Use RBAC to restrict access to data according to user roles. Only designated admin roles will be able to update data.
- **Verification**: Verify logs for unwanted access attempts and confirm that only authorized roles may alter mission data.

2. Secure Data Transmission Using TLS

- **Asset**: Communication channels between ground control and spacecraft.
- **Threat**: Information Disclosure.
- **Narrative**: Sensitive directives might be revealed via intercepted conversations, endangering mission security.
- **Work Required**: Make sure that all data sent between spacecraft and ground control is encrypted using TLS.
- **Verification**: Verify that TLS is applied to all transmissions using packet inspection, and make sure that data cannot be intercepted while in transit.

3. Regular Audit Logs for User Activity

- **Asset**: User activity logs.
- **Threat**: Repudiation.
- **Narrative**: Malicious activity could go unnoticed without adequate recording, making it challenging to spot and track down unlawful activity.
- **Work Required**: Turn on logging for all important operations, particularly those involving data access and modification.
- **Verification**: Periodically check logs to make sure all actions are correctly documented, and evaluate log access limitations to guard against manipulation.