Assignment 01 – Rubric

Assignment 01 Rubric

This rubric is designed to assess the quality and depth of student responses for each task in **Assignment 01: Securing IoT Surveillance Airport Infrastructure**. The rubric emphasizes specificity, technical accuracy, and contextual application of concepts to ensure students avoid generic answers and demonstrate proficiency in design artifacts.

Task 1: Read the Paper (0 points)

- No submission required.

Task 2: Requirement Elicitations (10 points)

Objective: Develop a set of evil and security stories using business language contextualized with MQTT vulnerabilities within the study case environment.

Criteria	Excellent (10)	Good (8-9)	Fair (6-7)	Poor (0-5)
Alignment with MQTT vulnerabilities	Clearly identifies and integrates MQTT-specific vulnerabilities into both evil and security stories	Identifies some MQTT vulnerabilities, with mostly clear integration	Limited identification and integration of MQTT vulnerabilities	Little or no connection to MQTT vulnerabilities
Use of Business Language	Clear, concise, and domain-appropriate language used consistently	Mostly clear with minor lapses in business language	Business language inconsistently applied	Language is vague, generic, or unclear
Completeness of Stories	Provides multiple detailed evil and security stories with specific impacts on the system	Provides multiple stories with sufficient detail and impact	Provides limited stories with minimal detail	Stories are incomplete, vague, or missing

Criteria	Excellent (10)	Good (8-9)	Fair (6-7)	Poor (0-5)
Formatting and Standard Use	Fully adheres to the provided standard for story formatting	Mostly follows the provided standard with minor deviations	Partially follows the standard with noticeable deviations	Fails to follow the standard

Task 3: Architecture of the Problem Description using DFD (20 points)

Objective: Develop a Data Flow Diagram (DFD) using OWASP Threat Dragon to represent the system architecture and identify affected components.

Criteria	Excellent (20)	Good (16-19)	Fair (12-15)	Poor (0-11)
System Representation	Comprehensive and accurate DFD that clearly represents the system architecture	Clear DFD with minor inaccuracies or omissions	Basic DFD with noticeable inaccuracies or missing components	Poorly constructed DFD with minimal detail
Component Identification	Accurately identifies all components affected by evil and security stories	Identifies most affected components	Identifies some affected components	Fails to identify key components
Methodology Compliance	Fully applies the methodology taught in class, with proper symbols and conventions	Mostly applies the methodology, with minor deviations	Partially applies the methodology, with noticeable deviations	Does not apply the methodology correctly
Documentation in OWASP Threat Dragon	Detailed component descriptions provided in the OWASP Threat Dragon JSON file	Component descriptions mostly complete, with minor omissions	Limited component descriptions with missing details	Minimal or no component descriptions in OWASP Threat Dragon

Task 4: Threat Enumeration using STRIDE (40 points)

Objective: Enumerate threats using the STRIDE framework, supported by CAPEC, CWE, and CVE references, and contextualize them within the MQTT-based system.

Criteria	Excellent (40)	Good (32-39)	Fair (24-31)	Poor (0-23)
Contextual Relevance	Threat enumeration is fully contextualized within the MQTT-based system, avoiding generic threats	Mostly contextualized, with minor generic elements	Partially contextualized, with some generic threats	Largely generic threats with minimal context
STRIDE Framework Application	Correctly applies all STRIDE categories, using appropriate terminology	Correctly applies most STRIDE categories, with minor errors	Applies some STRIDE categories, with noticeable errors	Misapplies or omits STRIDE categories
Threat Enumeration Standard Usage	Fully follows the threat enumeration standard, including source, prerequisites, action, and impact	Mostly follows the standard, with minor deviations	Partially follows the standard, with some missing elements	Does not follow the threat enumeration standard
Use of CAPEC, CWE, and CVE	Correctly references CAPEC, CWE, and CVE entries to support threat descriptions	References relevant CAPEC, CWE, or CVE entries, with minor omissions	Limited or inconsistent use of CAPEC, CWE, or CVE references	Little or no use of CAPEC, CWE, or CVE references
Likelihood Assessment	Provides clear likelihood assessments for each threat, based on realistic scenarios	Provides likelihood assessments, with minor inaccuracies	Basic likelihood assessments with limited justification	Missing or unclear likelihood assessments

Criteria	Excellent (40)	Good (32-39)	Fair (24-31)	Poor (0-23)
Technical Explanation (PDF)	Detailed and clear technical explanations for each threat, citing CAPEC, CWE, or CVE entries	Clear explanations, with minor omissions or unclear references	Basic explanations, with minimal detail or missing references	Poorly explained threats with little technical detail

Task 5: Attack Flow (30 points)

Objective: Design an attack flow using MITRE Attack Flow to describe an attack exploiting MQTT, highlighting differences from the original Golden Cup exploitation.

Criteria	Excellent (30)	Good (24-29)	Fair (18-23)	Poor (0-17)
Attack Flow Design	Comprehensive and logically structured attack flow with clear sequences of adversary behaviors	Clear and mostly accurate attack flow, with minor inconsistencies	Basic attack flow with some unclear sequences	Poorly structured or unclear attack flow
MITRE Attack Flow Tool Usage	Correct use of the MITRE Attack Flow tool, with all required elements in the “afb” file	Mostly correct use of the tool, with minor omissions	Limited use of the tool, with missing elements	Incorrect or minimal use of the tool
Adversary Behavior Sequences	Clearly describes sequences of adversary behaviors, aligned with ATT&CK Navigator layers	Describes most behaviors accurately, with minor gaps	Basic description of behaviors, with limited detail	Minimal or unclear description of behaviors
Comparison with Golden Cup Exploit	Clearly explains differences from the original Golden Cup exploitation, with specific examples	Explains differences, with minor omissions	Basic comparison, with limited detail	Minimal or no comparison with the Golden Cup exploitation

Assignment 01 – Rubric

Criteria	Excellent (30)	Good (24-29)	Fair (18-23)	Poor (0-17)
Technical Explanation (PDF)	Detailed and clear one-page technical explanation, with well-supported analysis	Clear explanation, with minor omissions	Basic explanation, with limited detail	Poorly explained attack flow with minimal technical detail

Submission Requirements:

- Ensure that all files (Word, JSON, PDF, and afb) are submitted according to the instructions in each task.
- Use clear file naming conventions to facilitate grading.