PART ONE – Security Cards

What to do

1. Getting Started

Read the Aircraft Maintenance Scenario and download the **Security Cards PDF** from the assignment page. Use these cards to brainstorm threats.

2. Identify Human Impacts.

Using cards in the Human Impact dimension, you should identify SEVEN **different** ways that the system could potentially be used or abused to negatively impact direct and indirect stakeholders.

Consider these Human Impact cards:

1. Emotional Wellbeing.
2. Financial Wellbeing.
3. Personal Data.
4. Physical Wellbeing.
5. Relationships.
6. Societal Wellbeing.
7. The Biosphere.

For each card, answer the questions on the card with respect to a stakeholders. A stakeholder is defined by NIST as “An individual, team, organization, or classes thereof, having an interest in a system.”

When answering the questions, keep your answers to one or two sentences. For example, a very good answer for Human Impact of threats to a voting system might be “Societal Wellbeing -- Trust in democracy is damaged by widespread damage to the integrity of the voting”.

3. Identify Threats to the System.

Explore SEVEN potential **different** threats to the system, where a threat is defined as a potential action from an adversary.

Consider each Human Impact identified in the previous step and generate a potential threat by selecting a set of cards; the set should contain cards from at ALL dimensions (e.g., Adversary's Motivations, Adversary's Resources, and Adversary's Method’s) and answering the questions on each card.

For example, a very good answer for threats to a voting system might be:

- Threat: Nation State bribes voters to elect their candidate.
- Motivation (Politics): An adversary might influence voters to vote for their candidate. The adversary could be an Nation State wishing to put in place a friendly candidate who will give them a break on trade deals.
- Resources (Money): Large amounts of cash might be available because the adversary is a Nation State. The amount of cash influences how many bribes ban be paid and the overall effect on the election.

- Method (Manipulation or Coercion) The adversary manipulates the public by paying them to vote for their candidate. By having enough votes to elect the candidate the overall integrity of the election is compromised.

This is a good answer because it tells me the cards considered, answers the questions on each of the cards, provides concrete details relevant to the scenario and the answers are consistent with each other.

4. Identify the Most Relevant Threats to the System

Identify the THREE most relevant threats to the system.

Define what you mean by “relevant” and discuss why you chose these threats to the system as most relevant.

Note that there is no "right" nor "wrong" ordering based on relevance. Each person might interpret "relevance" differently - for example, realism of attack attempt vs. likelihood of attack success vs. effect of successful attack.

5. Propose How to Mitigate the Threats

Provide a short dicussion for each of the THREE threats on mitigations to the threats identified above.

- You should have three different mitigations.
- Each mitigation should be explained using a two or three sentences and relate to scenario, for example simply saying “Sign the message” would be insufficient because we don’t know what message and how this mitigates a given threat.
- Consider any negative effects of implementing the mitigation. Write no more than half a page overall.

What to submit

Submit your answers as a PDF.

You MUST follow the template provided on the assignment page to make it easier for the marker to assess your work.

Submit your answers as **security-cards.pdf** via the ECS submission system.

Grading

You will be graded out of 100 marks based upon completeness and correctness.

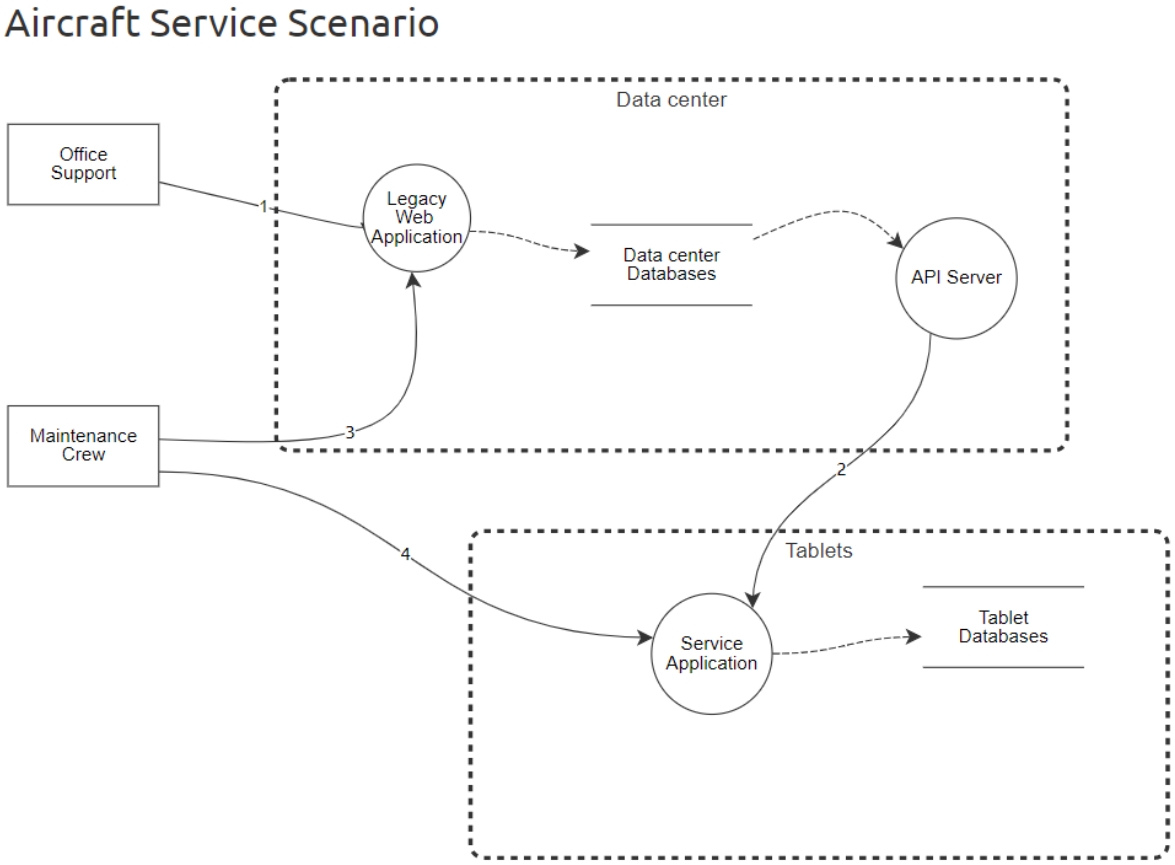
You will gain more marks for answers that are specific to the scenario rather than purely generic.

Please check spelling, understandability, and use full sentences.

PART TWO – STRIDE

0. Getting Started.

Review the DFD for the Aircraft Service Scenario and the following security assumptions.



You can assume the following:

- Data center is actually an office in the airport and is accessible by any Office Support staff or Maintenance Crew.
- Office Support and Maintenance Crew interact with the Legacy Web Application over HTTP via browser.
- Legacy Web Application uses a simple authentication scheme similar to that shown in CYBR171 where a username and password is sent and a cookie on the client side to track “logged in” state.
- Service Application interact with the API Server over HTTP using a REST protocol (the key point being that a browser is not used at all and data is just sent and received as plaintext between the processes).
- Maintenance Crew interact with the Service Application directly via the tablet’s touchscreen.
- Android tablets are not protected by any lockscreen and the same Google ID and password is used by all Maintenance Crew. This has led to games and other applications being installed by staff on the tablets.
- Legacy Web Application and API Server dataflows connecting them to the Data Center Databases is trusted as is the Service Application dataflow connecting it to the Tablet Databases.

- The Data Center Databases and Tablet Databases are not protected at all in term of access or encryption.

2. Perform a STRIDE-per-element analysis of the diagram

We have provided a template on the assignment page. Complete the tables to identify a range of different threats. The template is organised by DFD element and requires you to specify the following:

- Description of the threat and its impact upon the security of the system.
- Mitigation for the threat and how it will act to mitigate the threat.

We have limited the number of threats and asked you to provide only one description of a type of threat for a given element, e.g.. only one description of a denial-of-service threat to the Service Application rather than multiple ones.

You will gain more marks for providing a range of different threat descriptions for each instance of a type of element for a particular type of threat (where possible), e.g. aim to have a different threat description and mitigation for tampering with the Data Center database and the Tablet database.

You may want to refer back to your Cybersecurity Fundamentals notes on cryptography, applications of cryptography, what's wrong with passwords, viruses, wireless attacks, web security and social engineering.

What to submit

Submit your answers as a PDF.

You MUST follow the template provided on the assignment page to make it easier for the marker to assess your work.

Submit your answers as **STRIDE.pdf** via the ECS submission system.

Grading

You will be graded out of 100 marks based upon completeness and correctness.

You will gain more marks for answers that are specific to the scenario rather than purely generic.

Please check spelling, understandability, and use full sentences.