SurveyName E4_ExperimentSurvey

Consent This assignment will collect data on behalf of XXX University. The scientist in charge is XXXX.

 You are going to be asked if you agree that your ANONYMIZED answers in this experiment can be used for research and educational purposes and in particular it would be shared with your fellow MSc students in the course or PhDs to evaluate the success of the interventions. If you reply
        YES: The columns containing your name, surname, student ID, and email will be removed from the data before the rest of the data is shared .
        NO: The entire row (e.g. also the lines you selected as vulnerable) will be deleted when we will share the anonymised data with fellow students.
   The choice will have no impact on your evaluation. The full consent form is available via this link. You can also withdraw the consent at any time by contacting the teacher and the scientist in charge.

 The columns containing your personal details (name, surname, student ID, and email) will only be used by the teachers to attribute to you the credits of the active participation in the experiment.

Q79 Do you agree that your ANONYMIZED answers in this experiment can be used for educational and research purposes? Including processing by your fellows.

○ Yes (4)

○ No (5)

Page Break ─────────────────────────────────────

Welcome

You have already received;
1. A lecture on threat analysis using STRIDE.
2. A short scenario description of modifying and updating repositories on GitHub.
3. A short description of a pod deployment on Kubernetes.

 In this Experiment;
 You will also be presented with a list of security threats to each scenario separately. You will be asked to mark the threats for correctness (i.e., assess whether the threat is realistic or is a bogus/unrealistic threat).

Please, use only the survey buttons to navigate the survey (do not use the browser buttons).

Experimental procedure:
1) In the first part (Block 1) - you will find again a link to the scenario descriptions (a word document description is also provided). You will also be presented with a list of threats and decide on each threat about its correctness. Mark ONLY the threats you assessed as being correct/realistic.

2) You will then receive the second scenario, repeat the same procedure as above in the second scenario.

3) At the end of the survey, we will ask a few additional questions about the task (Block 2), your background (Block 3), and about the process of the experiment (Block 4).

 After 1h:45min you should be done with the task and will be automatically moved to the end of the survey.

Happy threat analyzing!

Page Break ⸺

StudentID Fill in your first name, last name, and student ID.
Example
First Name: XXXX
Last Name: XXXX
Student ID: 1234567
Email Address: XXXX

○ First Name (4) _____

○ Last Name (5) _____

○ Student ID (6) _____

○ Email (8) _____

Page Break ————————————————————————————————————

Q36 You will receive a confirmation email to ${StudentID/ChoiceTextEntryValue/8}
Is this correct?

○ Yes (1)

○ No (then go back and fix it) (2)

GroupA
Which group were you assigned to?

○ Group A (4)

○ Group B (5)

○ Group C (10)

○ Group D (11)

End of Block: Welcome

JS

Q25 Timing
First Click (1)
Last Click (2)
Page Submit (3)
Click Count (4)

ChatGPT DFD Note ** This study requires a chatGPT account, If you don't have an account, please raise your hand, the TA will help you create one**

 1.1 Follow the links to;
 The scenario: - GitHub scenario (Please open in a new tab)
 The walkthrough (Please open in a new tab)

  IMPORTANT: Please do not share this video with other students that belong to another group!

  1.2 Here is a word document of the scenario you just watched: Scenario Description and the Scenario training slides

 In this section, promt ChatGPT to assess the correctness of each threat, separately. That is, paste each threat separately and query the LLM to answer whether an actual security exists or not.

 2. Please log in to ChatGPT here.

 3. Copy and Paste each threat separately and query the LLM to assist you in assessing its correctness. Start a new chat, on the LLM, for each threat
     List of Threats (Please open in a new tab)

 4. Using the advice from ChatGPT, decide which of these threats are applicable* (mark **ONLY** the threats you assess as applicable)

5. For each threat marked as realistic, please provide your justification for why you marked it as being realistic. Paste the link to the chat with chatGPT in the text box below each threat ID (as shown in the walkthrough video)

Note*: Correct applicable threats are security threats that are realistic and pose an actual threat to the system. This means that the attack scenario can technically be carried out (i.e., the attack is feasible). In addition, if any threat-related assumptions are made, they must not contradict the case description in any way.

☐   1. STOLEN-AUTH-INFO (4)

_____

☐   2. LEAKED-CONFIG-FILE (5)

_____

☐   3. DOS-SERVER (6)

_____

☐   4. MALICIOUS-CODE-GITHUB (7)

_____

☐   5. ELEVATION-PRIVILEDGED-ACCESS (8)

_____

☐   6. DOS-REMOTE-REPO (9)

_____

☐   7. DISCLOSE-THIRD-PARTY (10)

_____

☐   8. ELEVATION-PRIVILEDGED-REPO (11)

_____

☐   9. ELEVATION-PRIVILEDGED-CODE (12)

_____

☐   10. EXPLOIT-HTTP-PROTOCOL (13)

_____

Q66 To what extent do you think ChatGPT was useful in assessing applicable threat?

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

End of Block: Group A GitHub and GPT

Start of Block: Group A K8 and GPT

GA-ChatGPT K8 Note ** This study requires a chatGPT account, If you don't have an account, please raise your hand, the TA will help you create one**

1.1 Follow the links to;
The scenario: - Kubernetes scenario (Please open in a new tab)
The walkthrough (Please open in a new tab)

IMPORTANT: Please do not share this video with other students that belong to another group!

1.2 Here is a word document of the scenario you just watched: Scenario Description and the Scenario training slides

In this section, promt ChatGPT to assess the correctness of each threat, separately. That is, paste each threat separately and query the LLM to answer whether an actual security exists or not.

2. Please login to ChatGPT here.

3. Copy and Paste each threat separately and query the LLM to assist you in assessing its correctness. Start a new chat, on the LLM, for each threat
   List of Threats (Please open in a new tab)

4. Using the advice from ChatGPT, decide which of these threats are applicable* (mark **ONLY** the threats you assess as applicable)

5. For each threat marked as realistic, please provide your justification for why you marked it as

being realistic. Paste the link to the chat with chatGPT in the text box below each threat ID (as shown in the walkthrough video)

 Note*: Correct applicable threats are security threats that are realistic and pose an actual threat to the system. This means that the attack scenario can technically be carried out (i.e., the attack is feasible). In addition, if any threat-related assumptions are made, they must not contradict the case description in any way.

☐   1. LEAKED-PRIVILEGE-REMOTE (4)

_____

☐   2. SPOOFING-AUTH-WORKLOAD (5)

_____

☐   3. DOS-WORKERNODE (6)

_____

☐   4. ELEVATION-PRIVILEGE-MALICIOUS-IMG (7)

_____

☐   5. EXPLOIT-PRIVILEGED-CONTAINER (8)

_____

☐   6. PORT-JAMMING-NETWORK-POLICIES (9)

_____

☐   7. LEAKED-SECRET-DOCKERFILE (10)

_____

☐   8. CHAIN-ATTACK-MALICIOUS-INPUTS (11)

_____

☐   9. UNAUTH-CONFIG-TAMPERING (12)

_____

☐   10. SPOOFING-LAYER-3 (13)

_____

Q71 To what extent do you think ChatGPT was useful in assessing applicable threat?

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

End of Block: Group A K8 and GPT

Start of Block: Block 2: Perception Questions

Display This Question:

    If Which group were you assigned to? = Group A

    Or Which group were you assigned to? = Group C

JS

PerceptionA 2.1 How do you rate the usefulness of the information sources (in the handout material) you were given for the task (that is, marking correct applicable threats)?

	1 (useless) (1)	2 (somewhat useful) (2)	3 (neutral) (3)	4 (useful) (4)	5 (very useful, could not do without) (6)
Case description (4)	○	○	○	○	○
Sequence diagram (5)	○	○	○	○	○
DFD (6)	○	○	○	○	○
Threat description (7)	○	○	○	○	○
Threat category (8)	○	○	○	○	○
Threat assumptions (9)	○	○	○	○	○
Affected components (10)	○	○	○	○	○
ChatGPT (13)	○	○	○	○	○

Display This Question:

If Which group were you assigned to? = Group B

Or Which group were you assigned to? = Group D

JS

PerceptionB 2.2 How do you rate the usefulness of the information sources (in the handout material) you were given for the task (that is, marking correct applicable threats)?

	1 (useless) (1)	2 (somewhat useful) (2)	3 (neutral) (3)	4 (very useful) (4)	5 (very useful, could not do without) (11)
Case description (1)	○	○	○	○	○
Sequence diagram (2)	○	○	○	○	○
Threat description (3)	○	○	○	○	○
Threat category (4)	○	○	○	○	○
Threat assumptions (5)	○	○	○	○	○
Affected components (6)	○	○	○	○	○

JS

Familiar GitHub 2.3 You were sufficiently familiar with GitHub to execute the task

○ Strongly disagree (4)

○ Disagree (5)

○ Neutral (6)

○ Agree (7)

○ Strongly agree (8)

JS

Familiar Kubernetes 2.4 You were sufficiently familiar with Kubernetes to execute the task

- ○ Strongly disagree (4)

- ○ Disagree (5)

- ○ Neutral (6)

- ○ Agree (7)

- ○ Strongly agree (8)

FamiliaritySTRIDE 2.5 You were sufficiently familiar with the STRIDE threat categories to understand the threat descriptions.

- ○ Strongly disagree (4)

- ○ Disagree (5)

- ○ Neutral (6)

- ○ Agree (7)

- ○ Strongly agree (8)

PerceivedCorrect 2.6 Rate the difficulty of marking the correct applicable threats.

○ Very Easy (1)

○ Easy (2)

○ Neutral (3)

○ Hard (4)

○ Very Hard (5)

Process.Correct 2.7 Rate your confidence that your solution is correct.

○ 0-20% (1)

○ 20-40% (2)

○ 40-60% (3)

○ 60-80% (4)

○ 80%-100% (5)

Group B DFD noGPT
1.1 Follow the links to;
The scenario: - GitHub scenario (Please open in a new tab)
The walkthrough (Please open in a new tab)

IMPORTANT: Please do not share this video with other students from another group!

1.2 Here is a Word document of the scenario you just watched: Scenario Description and the Scenario training slides

Mark the correct applicable threats* in the list of threats linked to this file. In the text box below each threat, please provide a short justification for the threats you assessed as being realistic

(Please open in a new tab)

Note*: Correct applicable threats are security threats that are realistic and pose an actual threat to the system. This means that the attack scenario can technically be carried out (i.e., the attack is feasible). In addition, if any threat-related assumptions are made, they must not contradict the case description in any way.

☐   1. STOLEN-AUTH-INFO (15)

☐   2. LEAKED-CONFIG-FILE (5)

☐   3. DOS-SERVER (6)

☐   4. MALICIOUS-CODE-GITHUB (7)

☐   5. ELEVATION-PRIVILEDGED-ACCESS (8)

☐   6. DOS-REMOTE-REPO (9)

☐   7. DISCLOSE-THIRD-PARTY (10)

☐   8. ELEVATION-PRIVILEDGED-REPO (11)

☐   9. ELEVATION-PRIVILEDGED-CODE (12)

☐   10. EXPLOIT-HTTP-PROTOCOL (13)

End of Block: Group B GitHub

Group B K8 noGPT 1.1 Follow the links to;
 The scenario video: - Kubernetes scenario (Please open in a new tab)
 The walkthrough (Please open in a new tab)

 IMPORTANT: Please do not share this video with other students from another group!
  1.2 Here is a Word document of the scenario you just watched: Scenario Description and the
Scenario training slides

 Mark the correct applicable threats* in the list of threats linked to this file. In the text box below
each threat, please provide a short justification for the threats you assessed as being realistic

 Kubernetes - List of Threats (Please open in a new tab)

Note: Correct applicable threats are security threats that are realistic and pose an actual threat
to the system. This means that the attack scenario can technically be carried out (i.e., the attack
is feasible). In addition, if any threat-related assumptions are made, they must not contradict the
case description in any way.*

☐   1. LEAKED-PRIVILEGE-REMOTE (15)
_____

☐   2. SPOOFING-AUTH-WORKLOAD (5)
_____

☐   3. DOS-WORKERNODE (6)
_____

☐   4. ELEVATION-PRIVILEGE-MALICIOUS-IMG (7)
_____

☐   5. EXPLOIT-PRIVILEGED-CONTAINER (8)
_____

☐   6. PORT-JAMMING-NETWORK-POLICIES (9)
_____

☐   7. LEAKED-SECRET-DOCKERFILE (10)
_____

☐   8. CHAIN-ATTACK-MALICIOUS-INPUTS (11)

_____

☐   9. UNAUTH-CONFIG-TAMPERING (12)

_____

☐   10. SPOOFING-LAYER-3 (13)

_____

End of Block: Group B K8

Start of Block: Block 3 Background

Q70 Thank you for answering the questions thus far. Next, we will ask you some questions about your personal background.

Gender What gender do you identify with?

◯ Male (4)

◯ Female (5)

◯ Non-binary (6)

◯ Other (please specify) (7)

_____

Age What is your age?

- ○ Under 18 (4)

- ○ 18-20 (5)

- ○ 21-24 (6)

- ○ Above 25 (7)

X→

Nationality What is your Nationality? Choose the country that coincides with your ethnic/cultural background

▼ Afghanistan (1) ... Click to write Choice 194 (1358)

---

study program Please indicate your study program:

- ○ Artificial Intelligence Systems (1)

- ○ Bioinformatics and Systems Biology (2)

- ○ Computer Science (3)

- ○ Information Science (4)

- ○ Computer Security (5)

- ○ Other (please specify) (6)

  _____

End of Block: Block 3 Background

Start of Block: Block 4 : Process Questions

Process.Understand 3.1 You had a clear understanding of what the task asked you to do?

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Process.Time 3.2 You were given sufficient time to read the material and complete the task.

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Process.Training 3.3 The training video prepared you sufficiently to carry out the task.

○ Strongly disagree (1)

○ Disagree (2)

○ Neutral (3)

○ Agree (4)

○ Strongly agree (5)

Process.remarks 3.4 If you have additional comments or remarks on this experiment, please enter the here (optional):

_____

_____

_____

_____

_____

End of Block: Block 4 : Process Questions