LLM for threat validation-Upwork A

Start of Block: Welcome

SurveyName Threat Validation- This survey is not fully compatible with mobile browsers, please open it on a PC browser

Consent This experiment will collect data on behalf of Vrije Universiteit Amsterdam, the Netherlands. The scientist in charge is Dr. Katja Tuma. This survey has been approved by the VUA Ethics Board. 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 PhD candidates to evaluate the success of the interventions. If you reply YES: Any personally identifiable information (PII) will be removed before the rest of the data is shared/analysed. NO: Your responses will be removed/not considered during data analysis. The full consent form is available via this link. You can also withdraw the consent at any time by exiting/closing this survey.

Q79 Do you agree that your ANONYMIZED answers in this experiment can be used for research purposes?

- ○ Yes (4)
- ○ No (5)

Page Break

Welcome
You have already received;
1. A lecture on threat analysis using STRIDE (You can watch the lecture again here)
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 (We define a correct threat as that which is likely to occur regardless of the residual impact; high, medium, low).

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 personal 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!

End of Block: Welcome

Start of Block: Group A GitHub and GPT

ChatGPT DFD Note ** This study requires a chatGPT account** 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: Github scenario 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 (Opens 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 (open a new chatGPT chat for each threat ID) 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. We define a correct threat as that which is likely to occur regardless of the residual impact; high, medium, low.

- [ ] 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)

Q89 Please provide your justification for why you marked it as being realistic or not. Paste the link to the chat with chatGPT (as shown in the walkthrough video)

	Justification (1)	chatGPT link (2)
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** 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: K8s scenario 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 (Opens 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. We define a correct threat as that which is likely to occur regardless of the residual impact; high, medium, low.

- [ ] 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)

Q82 Please provide your justification for why you marked it as being realistic or not. Paste the link to the chat with chatGPT in the text box below each threat ID (as shown in the walkthrough video)

	Justification (1)	chatGPT link (2)
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

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)	○	○	○	○	○

JS

Familiar GitHub 2.2 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 2.3 You were sufficiently familiar with Kubernetes to execute the task

- Strongly disagree (4)
- Disagree (5)
- Neutral (6)
- Agree (7)
- Strongly agree (8)

FamiliaritySTRIDE 2.4 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 2.5 Rate the difficulty of marking the correct applicable threats.

- Very Easy (1)
- Easy (2)
- Neutral (3)
- Hard (4)
- Very Hard (5)

Process.Correct 2.6 Rate your confidence that your solution is correct.

- 0-20% (1)
- 20-40% (2)
- 40-60% (3)
- 60-80% (4)
- 80%-100% (5)

End of Block: Block 2: Perception Questions

Start of Block: Block 3 : Demographics

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

Gender 3.1 What gender do you identify with?

- ○ Male (4)
- ○ Female (5)
- ○ Non-binary (6)
- ○ Prefer not to say (7)

Age 3.2 What is your age?

- ○ Under 25 (4)
- ○ 25 - 35 (5)
- ○ 36 - 45 (6)
- ○ Above 45 (7)

X→

Nationality 3.3 What is your Nationality? Choose the country that coincides with your ethnic/cultural background

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

Q93 3.4 What is your current role (professional occupation)?

- ○ System Administrator (1)
- ○ Devops Engineer (2)
- ○ Software Architect (3)
- ○ Software Engineer (4)
- ○ Product Manager (5)
- ○ Quality Assurance/Tester (6)
- ○ Security Manager (7)
- ○ Other (Please specify) (8) _____

Q94 3.5 How long have you been working in this role?

- ○ Less than a year (1)
- ○ 1- 5 years (2)
- ○ 6 - 10 years (3)
- ○ 10 - 20 years (4)
- ○ More than 20 years (Please specify) (5) _____

End of Block: Block 3 : Demographics

Start of Block: Block 4 : Process Questions

Process.Understand 4.1 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 4.2 How long did it take you to read the material provided (including watching the training video)

_____

Process.Training 4.3 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 4.4 If you have additional comments or remarks on this experiment, please enter the here (optional):

_____

_____

_____

_____

_____

profile 4.5 Kindly leave your Upwork profile below for the ease of processing payments

_____

End of Block: Block 4 : Process Questions