Hot Java

Findings and Reporting Information Console (FRIC)

Interview Report

Version 1.1.4

02/15/2020

Document Control

Approval

The Guidance Team and the customers will approve this document.

Document Change Control

Initial Release	2.0
Current Release	3.0
Indicator of Last Page in Document	$
Date of Last Review	02/15/2020
Date of Next Review	02/15/2020
Target Date for Next Update	02/22/2020

Distribution List

This following list of people will receive a copy of this document every time a new version of this document becomes available:

Guidance Team Members: Ms. Elsa Tai Ramirez and Mr. Ben Robertson

Customer: Cyber Experimentation & Analysis Division (CEAD)

Software Team Members: Joaquin Hidalgo (System Analyst), Fernando Marquez (System Architect), Lauren Eagan (Designer), Cynthia Sustaita (Lead Programmer), and Jesus Gutierrez (V & V Supervisor).

Change Summary

The following table details changes made between versions of this document

Version	Date	Modifier	Description
1.0	02/07/2020	Hot Java	Met as a team and assigned individual sections of audio recordings for transcriptions.
1.0.1	02/13/2020	Cynthia Sustaita	Added 'General Questions' and ''Users' questions from interview to report
1.0.1	02/13/2020	Jesus Gutierrez	Breakdown of tasks into sections
1.0.2	02/13/2020	Fernando Marquez	Added purpose (Section 1)
1.0.2	02/13/2020	Joaquin Hidalgo	Condensed feedback from level 2 use case and Q & A
1.0.3	02/13/2020	Lauren Eagan	Edited sections 1.1 - 1.3
1.0.4	02/14/2020	Joaquin Hidalgo	Added the following sections into 3.3: - 3.3.1 Related to task - 3.3.2 Related to findings - 3.3.3 Related to how progress is measured - 3.3.4 Related to how to generate a report Answered 'Task/Subtask' questions: - #15
1.0.5	02/14/2020	Jesus Gutierrez	Modified section 1.1 project overview Added following answers to questions 3.a.iii
1.0.6	02/14/2020	Cynthia Sustaita	Answered 'User's Questions from section 2.1: - #3 and 4.a

			Made comments throughout the document for review/feedback purposes. Added all of the remaining interview questions into section 2.1 Added Appendices descriptions. Added 10:30-11:50 individual transcription into appendix B
1.0.7	02/15/2020	Jesus Gutierrez	Added 7:30-8:50 individual transcription into appendix A Added 10:30-11:50 individual transcription into appendix B Added 2:00-4:00 individual transcription into appendix C Added section 1.2
1.0.8	02/15/2020	Cynthia Sustaita	Added individual transcriptions into Appendix A and C. Answered questions 43.a and 43.b Edited section 3.5 Edited Distribution List
1.0.9	02/15/2020	Lauren Eagan Cynthia Sustaita Jesus Gutierrez	Cleaned appendices in terms of font and structure
1.1.0	02/15/2020	Joaquin Hidalgo	-Edited section 3.3 based on Elsa’s feedback in regards to new questions for client - Added transcriptions Appendix A (33:00 – 48:00) - Added transcriptions Appendix B (42:00 – 56:00) - Added transcriptions Appendix B (Recording #4)
1.1.1	02/15/2020	Cynthia Sustaita Lauren Eagan Joaquin Hidalgo Fernando Marquez	Added summarized answers to section 2.1

1.1.2	02/15/2020	Fernando Marquez	Edited section 3.3 based on Elsa’s feedback in regards to new questions for client - Added transcriptions Appendix A (1:04:00 - 1:21:00) - Added transcriptions Appendix B (88:00 - 110:00) - Added transcriptions Appendix C (Recording #5 and #6)
1.1.3	02/15/2020	Joaquin Hidalgo	Added inconsistencies obtained from RDD to interview sessions
1.1.4	02/15/2020	Hot Java	Moved questions into section 3 Reviewed report as a team before submission. Answered sections 3

Table of Contents

Document Control **3**

Purpose **6**

Project Overview 6

Background and Contact Information of Interviewee 6

Interview Information 6

References 6

Interview: Questions and Responses **7**

Prepared Questions and Responses 7

Additional Information 13

Action Items **14**

Inconsistencies 14

Unclear Items 14

New Questions 14

Unanswered Questions 14

Next Steps 14

Appendix A **23**

Appendix B **45**

Appendix C **62**

1. Purpose

The purpose of this report is to describe and document the details of the client's interview. The interview established the overall goal of the project, use of the system, and functionality of the system. Information in regards to data and services was gathered through a set of requirement questions that we, as a team, came up with after analyzing the RDD. This interview not only provided us with clarifications and suggestions on how the system could be created, but it will also serve the purpose of informing our client about what our understanding of the system is. Overall, our intention is for this document to allow the clients to guide us through the path needed for us to fulfill the requirement of the project as efficiently and successfully as possible.

1.1. Project Overview

Our motivation in creating this project is to provide a useful and efficient system for users to document and efficiently store findings in an organized manner in regards to cyber vulnerabilities experiments as well as provide mitigations recommendations. The system will aid a CEAD lead analyst to come up with tasks, and subtasks as well to assign them to CEAD analysts. The system will also be allowed to have multiple analysts that are able to sync data together in order to complete the given assessment as a team. The team will be able to keep track of the work of the users that will allow the status of progress to the system. Tasks will be viewed with a visual chart.

1.2. Background and Contact Information of Interviewee

As part of the Department of Defense (DOD) Technology Combat Systems Acquisition Process team, our interviewee's are as follows:

a. Dr. Oscar Perez: *oscar.a.perez46.civ@mail.mil*
b. Mr. Juan Ulloa: *juan.j.ulloa.civ@mail.mil*
c. Mr. Angel Avila: *angel.e.avila2.civ@mail.mil*

1.3. Interview Information

The interview was facilitated by Ms. Elsa Tai Ramirez, the course lecturer. Each of the Software Engineering teams had a representative reading questions from an assigned section. There were two different interview sessions:

Date: Thursday, February 6, 2020
Time: 7:30 – 8:50 a.m. and 10:30 – 11:50 a.m.
Place: UTEP Chemistry and Computer Science Building RM 1.0202

Additionally, there was an extra session which was only conducted by Ms. Elsa Tai Ramirez outside of class time. Its results were provided to every Software Engineering tema via recordings

(Appendix C):

Date: Thursday, February 6, 2020
Time: 7:30 – 8:50 a.m. and 10:30 – 11:50 a.m. 2:00 - 4:00 p.m
Place: UTEP

1.4. References

Client Interview Audios. The University of Texas at El Paso, Chemistry and Computer Science Building 1.0202.

O. Perez, H. Vasquez, T. Provencio, J. Rivers, A. Cuevas, and V. Fonseca, "RDD - Findings and Reporting Information Console (FRIC)." .

H. Vasquez, V. Fonseca, A. Cuevas, and J. Rivers, "Client Presentation," in Client Presentation, 06-Feb-2020.

2. Interview: Questions and Responses

In this section, there will be an overview of all questions and responses throughout the interview. In section 2.1, is the prepared list of questions as well as a summarization of the answers given. In section 2.2, any additional information outside of the formal questions and responses can be found. Furthermore, in the Appendix section of this report, the official transcription of our interview session as well as two others can be found in this order: Appendix A, the session from 7:30-8:50 a.m., Appendix B, 10:30-11:50 a.m., Appendix B from 2:00-4:00 p.m..

2.1. Prepared Questions and Responses

General questions

1. Please describe the current process used to collect information during a cyber engagement.
   - *i.* *It is stated that during a cyber engagement, CEAD cyber analysts work cooperatively with the Project Manager and Subject Matter Experts. The current process to collect information during a cyber engagement starts with the analyst specifying the system and internal tools going to be used. This helps by defining the scope to understand the bounds of the system. The system is flexible and can be used in different ways thus establishing the rules with team needs to be done. After the rules are set and analysts begin to work, as they use their tools to gather findings, it's important for the system to communicate with each other to share findings by collecting pictures, text and then syncing their data.*

2. Is there a solution that you are currently using? If so, please provide a list of dislikes regarding the current solution.
   - *i.* *Unanswered question*

Users

3. RDD stated that there are two types of users: Lead analyst and analyst.
   a. Please elaborate on the difference between a lead analyst and analyst about their privileges:
      - i. (Appendix B - 0:19:07) *The lead analyst will be the user receiving updates when it comes to what the current progress is, what hasn't been completed as well in regards to any additional findings that have been discovered.*
      - *ii.* *The analyst will be the user performing the tasks that have been assigned to them. During this process, the analyst will maintain a record of what they have done, what has and hasn't been found in such a task.*

b. How will the system differentiate between the two?

i. (Appendix B- 0:21:38) *The system does not have a need to differentiate between the lead analyst and analyst as they both have admin privileges; this system will be a trust environment. However, the lead analyst will*

c. What would be a typical scenario of use by a lead analyst and by an analyst be?

i. The client provided us with two scenarios for each of these users:

1. (Appendix B - 0:23:48) A typical scenario of use by a lead analyst would be assign tasks to analysts after reviewing the list of analysts, then require these analysts to sync the data with them: the lead analyst.

2. A typical scenario of use by an analyst would be get assigned a task or list of tasks, work on such assignment, then report its current progress, sync to any other analyst (including the lead), and if necessary, create subtasks.

d. Are there further privileges for these user types not mentioned in the RDD?

i. (Appendix B - 26:10) No, there are no further privileges for these user types.

e. Are there other types of users not mentioned in the RDD?

i. (Appendix B - 0:26:13) No, there wouldn't be any other users other than the ones mentioned in the RDD: Lead and non-lead analysts.

4. How many lead analysts are allowed per cyber engagement?

i. (Appendix B - 0:26:20) An example scenario was a cyber engagement in Ft. Bliss required a number of 10 to 15 analysts. Therefore, the number of lead analysts allowed in an engagement would depend on the size of the scope (E.g. having a big network)

b. If only one lead analyst is allowed per cyber engagement, what should the system do if:

i. Unanswered question

c. The lead analyst retires from the engagement.

i. Unanswered question

d. The lead analyst demotes himself/herself to an analyst role.

i. Unanswered question

5. How should the analysts communicate within the project assuming the system supports an internal messaging system?

i. *Usually in the same room, open a chat system. Tasking system such as a ticketing system and set priority on tasks or subtasks*

6. What are the differences between lead analyst syncing and analyst syncing?

i. Both are able to push and pull data when syncing.

7. RDD stated that "A non-lead analyst can only view findings that they have not created". What is meant by this?

i. *By collaborating with an analys*t, *a non lead analyst can view the other analysts findings.*

8. How will an analyst/lead analyst be identified? What information will the system require from analysts? (E.g first name, last name, id)
    - i. *Names will not be used , but possibly a label (initials) or IP address. (Unclear answer to this question.)*
9. What analyst information do lead analysts have access to?
    - i. *(Appendix A - 50:500) Lead analysts have access to everything within the system.*

Technical Report

10. Do you want the system to represent some of the data in the technical report graphically? If so, please elaborate on the graphical data requirements.
    - i. *Unanswered question*
11. What are the export formats of the technical report?
    - i. *Unanswered question*
12. Should the technical report be sent directly to the project manager through the system or should it be exported as a file for the lead analyst to send at their discretion?
    - i. *It will be exported in an excel spreadsheet. (Partially unanswered)*
13. Please elaborate on the relationship between closing an event and the generation of the final report.
    - a. Does exporting the final report close the event?
        - i. *Unanswered question*
    - b. Does closing the event automatically generate a final report?
        - i. *Unanswered question*
14. What auditing requirements does the system have? (e.g. tracking exports, access/edit logs, other user records)
    - i. *Unanswered question*

Tasks/sub-tasks

15. Please provide a definition and example for the following concepts, describe the current process used to create them, and the relationship between them:
    - a. System:
        - i. (Appendix B - 42:01) *The system is a set defining of a system under test. It is what you are allowed and are not allowed to touch/test; This is your scope. (For example a certain IP address might be blacklisted, which means you cannot touch)*
    - b. Event:
        - i. (Appendix B - 42:40) *An event describes a natural assessment and penetration test depending on organization requirements from the DOT&E policy made by congress. An event is the dates that took place with the system. During an event, it is touching the system, doing*

vulnerability assessment of the system, collecting findings and is highly productive in reference to the analysts. The lead analyst will be the ones in communication with the clients and should be allowed to update the clients as needed.

   c. Task:
      i. (Appendix B - 44:10) *Task is the tools, applications or programs to assess the system on all or a set amount of systems. One or multiple tasks are needed to be done at an event which are the things that need to be completed by the analyst.*
   d. Subtask:
      i. (Appendix B - 45:06) *Subtask can be looking at the criticals and the highs from the assessments performed. Of the task or tools performed on a system, the subtask are the findings which are vulnerabilities, exploits or general data of what happened. Subtask can be to look at the critical findings and verify that the findings are true positives.*
   e. Finding:
      i. (Appendix B - 46:00) *Findings are vulnerabilities. It is possible to perform tasks but not have any findings. A finding will either lead to a true vulnerability or just a data point that is not a vulnerability but something that appeared to show the client. The team if can exploit a finding or gets very close to exploiting, the team talks about whether it's vulnerable or not and then declares it later on. Findings should also have a tag that makes this data set inputted as a vulnerable, informational or other, that way we can search by filter for these things. Findings don't need priority queues, it is just important to jot down the data with text or pictures as supporting evidence. Regardless, everything found will come out on the report to inform the end-client.*

16. Event:
   a. How long does an event last?
      i. *An event will generally last a week, this can be Monday to Friday but can also include the weekends on some occasions. (Appendix B 56:20)*
   b. What are "start" and "end" points?
      i. *The starting point is most often on Monday mornings and the ending point is usually Friday afternoons.*
17. Task
   a. What are the different status types that a task can be?
      i. *In this case, the decision of what status types are available will be left up to our team, the client asks that we research the best possible options and possibly include a ticketing system. For example: You have a task and somehow goes to the end. (Appendix B 56:47)*
   b. Can a task be created without an assignment to an analyst?
      i. *Yes, a task can be created without an assignment to an analyst (Appendix B 57:29)*

c. Is there a limit to backlogged tasks before new tasks can be created?

i. There is no limit (Appendix B 58:58)

d. What is the maximum number of subtasks that a task can have?

i. There is no limit (Appendix B 58:59)

e. What is the maximum number of images that can be attached to a task?

i. There is no limit (Appendix B 59:09)

f. What format do you want the due date displayed? E.g. MM/DD/YYYY, DD/MM/YYYY, or MM/DD/YYYY HH/MM.

i. *(Appendix B - 59:13) DDMMYYYY with no slashes to avoid confusion in linux systems.*

18. Please describe a scenario where a subtask is associated with more than one task (if applicable).

i. (Appendix B 1:02:00) Example scenario: There could be three tasks that are almost identical, or close to identical, but they're just being implemented to a different part of the network. You're going to have one task, that can be data collection, vulnerability assessment, etc. You would have to do it on ten hosts for the first task and another person would do it on another 10 hosts. Usually, the first day is information gathering, where everyone is doing the same tasks on a different section. On day two, using the information found, more tasks will be generated, or the team will be asked to help identify tasks.

19. Could a subtask be elevated to a task, and vice-versa?

i. (Appendix B 1:02:53) If a subtask is big enough, it can be elevated to task. Depending on if what the task is related to changes, having the flexibility to change it to a subtask would be appreciated.

20. Are there any constraints on the number of analysts to a task (sub-task)? If so, please specify the number constraint.

i. There are no constraints on the number of analysts to a task/subtask.

21. If there is an overdue task, how do you want the lead analyst to be notified? And how frequently should the lead analyst be notified?

i. An actual due date and progress

22. RDD stated that the lead analyst would be notified of due dates for tasks. Should the lead analyst also be notified when a task is complete?

i. (Appendix C - Recording 2 - 12:42) Implementing a notification that will alert them about a task being completed would be a nice feature

23. How is the priority being represented? (E.G. 1-5 Increasing in priority)

i. Some type of ranking system will be required, such as high, medium, low or 1, 2, 3.

24. Will the analyst/lead analyst be responsible for inputting all the necessary information regarding events/tasks/subtasks/findings to the system or will some of the information be imported from an external source?

i. Unanswered question

25. Should the system alert the non-lead analysts if the task their sub-task is linked to is completed? If yes, please elaborate on the preferred mechanism.
    i. *Unanswered question*
26. Should the system allow the lead analyst to swap non-lead analysts between tasks? If so, what should occur with their current assigned tasks?
    i. *(Appendix C Recording #3 - 18:57) Yes the task can be swapped because sometimes multiple analysts can be under a task with multiple subtasks and if one finished earlier than the other, one can help out their team mate to finish the task even faster. While sharing data between each other, if one analyst pulls, you don't delete any critical findings, you'd rather have duplicated and manually go through the findings to see what should stay and time stamps are required to know when the last thing was worked on. The lead in the particular event will either have the option make and edit rules to either delegate tasks or have the analyst define their own tasks/subtasks. (For example application: doors)*
27. Which aspects of the task are editable after the initial submission of the task or sub-task?
    i. *(Appendix C Recording #4 - 8:58) Everything is editable, no specific aspects.*
28. After an event is finalized, is it still possible to edit the event and the tasks and sub-tasks associated with it? If so, will this re-open the event?
    i. *(Appendix C Recording #4 - 9:25) Yes you can open it to view it and you can even edit it again to rewrite info/data for better clarification. You can also re-open the event to duplicate the event.. That data from one assessment doesn't appear in the new assessment because all the data from old events get saved into a hard drive which then the hard drive is uploaded to, Intel Bucket and then the hard drive gets reimaged. For the system, all the tasks and subtasks from the previous event are kept which then can be re-used for future use.*
29. Once a task has been completed, can an analyst go back and edit it or review it? Does the task disappear from the analysts' assigned tasks?
    i. *(Appendix C Recording #4 - 13:05) Already been covered.*
30. How is progress measured?
    i. *(Appendix C Recording #4 - 13:10) Progress is measured categorically by not started, in progress, completed for tasks/subtasks and the system. The lead analyst should see if people are creating tasks. Finding levels does not have status of progress but should be marked as vulnerability, informational or other. And possible to have the list of people of who did what as multiple people can take over a task/subtask if someone goes missing at work. (Ex. Elsa has assigned, Elsa completed, in progress, Juan not started, not do-able)*

Findings

31. Are the findings linked to each other under a sub-task or a task?
    i. *(Appendix C Recording #5 - 4:00) Findings should be attached to a subtask. You can make a task and attach a finding to it if no subtasks are there and then later on change that finding to a subtask. If subtask is there, then it must be attached to subtask. Findings can be linked to each other and be linked across different systems. When looking across all systems categorizing the findings, common findings will be clumped together.*
    (example: tire blew up, tire flat, tire dirty, can go into bucket of tire problems.) When talking to high level people, it should be easy to explain these categorized findings and when explaining to tech-e people, the technical issue and impact should be more detailed. (we should expect examples from the analyst like, "weak credentials")
32. What happens in the situation that an analyst is unable to detect a solution to a vulnerability?
    i. *There will be just no findings for that particular task*
33. Can a finding have more than one analyst as authors?
    i. *Collaborators*
34. Please elaborate on what you mean by "associate a finding to any other finding".
    i. *Basically group findings for system owner by grouping them by IP's*
35. Please define and provide examples of "data artifact".
    i. *JPEGs, PNGs and shadowing filing*
36. What if one of the findings is deleted, what should happen?
    i. *Depends sometimes criticality, archive it. Findings that are relevant go ahead and outbrief it. Give it scale of relevancy from 1 to 10.*
37. How will a discovered vulnerability outside the scope of a task or subtask be handled?
    i. *Unanswered question*
38. How does an analyst provide mitigation of a found vulnerability? Is it notes attached to the vulnerability documentation?
    i. *Unanswered question*
39. RDD stated that once a vulnerability is confirmed, a CEAD analyst must document this finding as well as mitigation so it can be added to the technical report when the event is done. It also stated that when a vulnerability is confirmed the analyst must mark the task

that is associated with the finding as complete so the lead analyst will have insight into the progress of the event.

   a. How does a vulnerability become confirmed, and is it possible for a vulnerability to become unconfirmed?
      i. *Unanswered question*
   b. In the case a vulnerability is unconfirmed, what should the software do with the information associated with that void vulnerability (findings, notes, description, etc)?
      i. *Unanswered question*

Searching/sorting

40. What search criteria does the system need to support?
      i. *Search criteria supported should be at minimum: By time, keyword, and analyst.*
41. What information is available to the lead analyst when searching for an analyst?
      i. *Unanswered question*
42. What information is available to an analyst when searching for an analyst?
      i. *Unanswered question*

Data Syncing

43. Please elaborate on the process of syncing data.
   a. What type of data can be shared between analysts and lead-analyst?
      i. *(Appendix A - 0:41:10) Since everybody has access to everything, both lead analyst and analyst will share all data.*
   b. What type of data can be shared between analysts?
      i. *(Appendix A - 0:41:10) Since everybody has access to everything, analysts are able to share all types of data between them.*
   c. How will data between analysts be synced with each other?

Data Storage

44. How will the data gathered by the system be stored? Will it be stored in a server, internal database, cloud service, or a distributed system?

        i. *The data will be stored in a hard drive and then archived.*

45. If the data will be stored in a database, please elaborate on the requirements for the database.
    a. If there are data exchanges between a pre-existing database, what language was used to create the database (sql/nosql)?
        i. *Unanswered question*
46. How much data is collected for each cyber engagement?
    a. What is the usual size and type of attachments being uploaded?
        i. *The size varies per attachment.*
    b. How long does the collected data need to be stored in the system after each cyber engagement?
        i. *Unanswered question*
47. Should there be a set of formatting and quality standards for images and non-image data artifacts, such as system and network scans, vulnerability validation, and penetration tests that are uploaded by the analysts? If yes, please elaborate on the formatting and quality requirements.
        i. *JPEGs, PNGs is the formatting generally used at this time.*
48. Does the system need to back up data? And if so, how often?
        i. *Unanswered question*

Graphical User Interface

49. Are there any constraints regarding the graphical user interface of the system?
    a. Should the system support a GUI interface or a terminal-based interface?
        i. *Unanswered question*
    b. Should the UI adapt to different screen sizes?
        i. *Unanswered question*
50. What format is needed for visual artifacts to maintain the fidelity that's required for accuracy?
        i. *Unanswered question*

Security

51. Would any type of authentication mechanism be required? If so, please elaborate on the authentication mechanism requirements.
        i. *Unanswered question*
52. What secure communication protocols should FRIC support?

i. *(7:16) SSH can be used to transfer data as opposed to sending clear text protocols.*

53. What level of encryption will the syncing process require?
    i. *Unanswered question*
54. Would the system be storing any sensitive data? If yes, what are the requirements for data protection?
    i. *Unanswered question*

Development Constraints

55. What languages would you want the system to be developed in? Please specify specific versions of programming languages (if applicable).
    i. *Possibly Python, but at this point in time it is not definitive.*
56. What operating system will the system be running on?
    i. *(9:23) At this time, the focus is on Linux, but compatibility to both Windows and Linux would be appreciated.*
57. What type of system will FRIC be implemented as? E.g. System application or web application.
    i. *(9:23) It is possible a web based system will be used, but has not been decided at this time.*
58. What considerations must we make regarding the maintenance of the system?
    i. *Unanswered question*
59. Will the system be used in a local computer network or will it allow users to access, communicate and transfer files through wireless connections? (Wi-Fi, Lan, etc.)?
    i. *(Appendix C) Yeah but more than likely, most of the time it's going to be a local and Lan*

2.2. Additional Information

In this section, any additional information not related to the questions asked formally in the interview will be added.

2.2.1. The lead analyst should be able to assign tasks specifically to an analyst as well as have an option to allow the analyst to pick their tasks.

2.2.2. When it comes to syncing, both the lead analyst and analyst are able to sync their data/current progress. However, since there's a risk of overwriting/deleting data, a feature to pull and push data would be appreciated.

2.2.3. Clients like the flexibility of their previous system as well as their lead analysts' ability to add new tasks

3. Action Items

3.1. Inconsistencies

In this section, we state any inconsistencies are the statements we obtain, understand and hear from any informational document or interview session as contradictions.

3.1.1. Related to tasks:

In the RDD it states that if you did not create the task, you are not allowed to edit or delete anything. In (Appendix C Recording #4 06:00) we are told that as long as you are a general analyst working under a task, you actually are allowed to edit or even delete certain findings while syncing data with each other which sounds better to have each analyst be given the power to choose what stays, what gets edited and what gets deleted.

3.1.2. Related to users:

Client first answered in question 3.e that there wouldn't be any other users other than the ones mentioned in the RDD: Lead and non-lead analysts. However, they admitted a contradiction as there can also be a team lead (Appendix B - 27:01).

3.2. Unclear Items

In this section, any responses that did not provide a definitive answer will be listed:

2. Is there a solution that you are currently using? If so, please provide a list of dislikes regarding the current solution.

Clients talked about the likings of their previous system (data redundancy, privileges). However, they did not mention what their dislikes were. (Appendix B-18:02)

8. How will an analyst/lead analyst be identified? What information will the system require from analysts? (E.g first name, last name, id)

Names will not be used , but possibly a label (initals) or IP address.

3.3. New Questions

In this section, we will add any questions that we formed from the information gathered in the interview sessions.

3.3.1. Related to task:

Should an analyst have the ability annotate the status of a task, regarding its progress? (i.e. in progress, not do-able, assigned to)

3.3.2. Related to Finding:

Would a function to keep a repository or record of findings be needed? (Example scenario: The analyst has a finding that may or may not be important, this analyst then saves the finding for possible later use, without attaching it to a task/subtask.)

3.3.3. Related to how progress how its measured:

Should we include that an assignment has been transferred to someone else because yeah it would be cool to say it's been transferred but it's not going to prevent someone from taking over the job. Then is it needed? Should our system have a history of created, in progress, completed for tasks/subtasks in sequential order with the overall status of that task/subtask.

3.3.4. Related to generate report:

Should we have a history or repository of the exported documents and to whom they were exported to in case an old report needs to be clarified that was given to a client.

3.4. Unanswered Questions

2. Is there a solution that you are currently using? If so, please provide a list of dislikes regarding the current solution.

4.b If only one lead analyst is allowed per cyber engagement, what should the system do if:

4.c The lead analyst retires from the engagement.

4.d The lead analyst demotes himself/herself to an analyst role.

10. Do you want the system to represent some of the data in the technical report graphically? If so, please elaborate on the graphical data requirements.

11. What are the export formats of the technical report?

12. Should the technical report be sent directly to the project manager through the system or should it be exported as a file for the lead analyst to send at their discretion?

13. Please elaborate on the relationship between closing an event and the generation of the final report.

a. Does exporting the final report close the event?

b. Does closing the event automatically generate a final report?

14. What auditing requirements does the system have? (e.g. tracking exports, access/edit logs, other user records)

24. Will the analyst/lead analyst be responsible for inputting all the necessary information regarding events/tasks/subtasks/findings to the system or will some of the information be imported from an external source?

25. Should the system alert the non-lead analysts if the task their sub-task is linked to is completed? If yes, please elaborate on the preferred mechanism.

37. How will a discovered vulnerability outside the scope of a task or subtask be handled?

38. How does an analyst provide mitigation of a found vulnerability? Is it notes attached to the vulnerability documentation?

39. RDD stated that once a vulnerability is confirmed, a CEAD analyst must document this finding as well as mitigation so it can be added to the technical report when the event is done. It also stated that when a vulnerability is confirmed the analyst must mark the task that is associated with the finding as complete so the lead analyst will have insight into the progress of the event.

a. How does a vulnerability become confirmed, and is it possible for a vulnerability to become unconfirmed?

b. In the case a vulnerability is unconfirmed, what should the software do with the information associated with that void vulnerability (findings, notes, description, etc)?

40. What search criteria does the system need to support?

a. By time
b. By keyword
c. By analyst.

41.What information is available to the lead analyst when searching for an analyst?

42.What information is available to an analyst when searching for an analyst?

46. How much data is collected for each cyber engagement?

a. How long does the collected data need to be stored in the system after each cyber engagement?

49. Are there any constraints regarding the graphical user interface of the system?

a.Should the system support a GUI interface or a terminal-based interface?
b.Should the UI adapt to different screen sizes?

50. What format is needed for visual artifacts to maintain the fidelity that's required for accuracy?

51. What level of encryption will the syncing process require?

53. What level of encryption will the syncing process require?

54. Would the system be storing any sensitive data? If yes, what are the requirements for data protection?

58. What considerations must we make regarding the maintenance of the system?

3.5. Next Steps

The next step in our project is to create a model to display our understanding of the system to the clients. As well as a memo in which we'd be setting up a meeting with our clients in order to ask a new set of questions based on these interviews, clarify inconsistencies as well as contradictions.

Appendix A

The following transcription was made based on an audio recording made by our classmates from the 7:30am - 8:50am section. It's structured in a way that readers are able to see who the speaker was among its corresponding timestamp.

Speaker 00:00-00:31: When was it? About 10 years ago, I am trying to remember her name in military. Who was it that took a lot of classified information and she is now like a representative?

Speaker 00:22: Chelsea Manning?

Speaker 00:23: Chelsea Manning. DOD just banned all use of pen brights or memory sticks or what do you call them now?

Speaker 00:37: USBs?

Speaker 00:38 USBs. So, unfortunately, we can't use a USB to copy a presentation but he's just going to email. Also, things about cyber security, back before cyber security, does anybody know what cyber security was called? What was known as or what the group was that big cyber security? Used to be called information assurance. So, people will say, I work in Information Assurance, and what do I do? Well I assure or ensure that information is secure. It's encrypted. It's protected. Everything. So pretty much everything that, that you guys are learning from cyber security. Specifically, that triad, who knows the cyber security triad? Three most fundamental basic things are the three umbrellas of cyber security. So, I'll give you three letters. It's CIA.

Speaker 01:42: I know the I is integrity.

Speaker 01:44: Integrity, very good. See, just guess. Confidence.

Speaker 01:56: Confidentiality? Availability.

Speaker 01:57: And availability. Very Good. So, back in the information assurance times, we've had five pillars. You have those three, and then you have two others. And I can't remember the fifth one, but I can remember the fourth one, which was it was called non-repudiation. What does that mean? What does non-repudiation mean? It means that when you do some type of process, right, you want to make sure you type that process in such a way so that the person that does something with that process can say, Oh, well, it wasn't me. I didn't use it. Because we know we have lives. We have whatever that they use them. So, you know, you can't say that you didn't do it. Anyways, I was just trying to entertain you.

Speaker Elsa 02:38: So, let me say thank you for coming to the class to do an interview with our students. We have Juan and Dr. Price here. Do you want to say a few words about yourself so that other classes are familiar with who you are?

Speaker Juan 02:51: Sure, a little startup, my name is Juan, I came to the university of Texas at El Paso, graduated back in 94. I taught for a few years, work for the water utilities, I actually my, my undergrad is in, in chemistry. When I was teaching, they opened up a new program for, for CS. And it was the first time, it was back in 2001. It was the first time when they would offer CS classes after work, because everything was always in the morning. So, like I jumped on and got a master's in computer science, and I'm now working for the army futures command. I've been working for the army for 15 years. Before that, or part of that I did a couple of internships. I worked at IBM for about four months. And I also went I got an opportunity to go up to our Berkeley National Labs and do an identity chip out there for three months. And I can just tell you how invaluable those opportunities were. And this is Dr.Perez and…

Speaker Oscar 03:48: Oscar Perez, I graduated in 2016 with my PHD over here from UTEP from the electrical engineering department. I After graduating in 2002, I started working over here at UTEP as a system administrator for the Undergraduate Learning Center. We usually, we used to take about 32 servers, 15 of them were like web servers to run out the audio visual, and, you know, different all the different projects that we have. After 2017 I moved to the army futures command, you know, as a cyber security analyst. How many attacks do you guys think that your UGLC gets, cyber attacks on a daily basis? Just take a guess.

Speaker 04:40 10000?

Speaker Oscar 04:41: Yeah, you're very close 10000. We have about 8000 attacks on the on the web servers that you have over there and so you always try to limit the surface by area that can be attacked. You design, I mean Monday, I was at New Mexico Tech recruiting, and then yesterday, Wednesday, I was at NMSU recruiting. So, where do you guys think I'm going to be tomorrow recruiting?

Speaker 05:07: Here.

Speaker Oscar 05:08: Over here at UTEP, so hopefully we can see some of you guys. Is this software engineering I or software engineering II? I? Perfect. So, by the time that you guys graduate, there's a high demand of computer scientists out there. I was talking to several people at the career fair, some other people that were recruiting too and I want to say probably, like 50% of the people recruiting were looking for computer science majors. And one of the big gaps that they have is cyber computer science majors that know about security, which I think this project will make you very marketable whenever you graduate because you'll have some security background after working on a tool like this. Actually, a one guy from one of the Air Force, Air Force bases that was recruiting he was telling me how computer science workers have stolen from different companies or even other, you know, DOD departments because you guys are very high demand. Mostly those of you that have a security background because those are hard to find. So all the certifications that you have to have if you want to, you know, work in the security field, or the CEH which is the Certified Ethical Hacker, the security plus and you know, the master of all things, see ISSP Okay, whenever you even if you don't take the certification, but if you start studying and seeing what the content of them are, people will start paying attention to you, people that are under security will. Now imagine with that number of attacks that we get over here at the university, imagine the number of attacks that we get as a Department of Defense, you know, there are a lot more. So, any every single department needs to have their systems secure and that's where you know all the people that have a secured background have come to play and the tool that you guys will be helping us build is precisely on that. Okay, we're going to go more in depth on this and this is not just a one-person effort is you know it is all of us and through the semester you guys will be working with Andy and the Beans, have they already met [Ben] and [Andy]? So right now, you know they could not be here they want to be here. But as we all got tell you a little bit of their job, is to go and assess different ARMY systems through the whole US. So sometimes we may be here in El Paso maybe next week. Actually, next week. I'm in Austin, and we got there we may be in Kentucky or California or Washington or, or Germany or Germany or Japan or you never know. But that's why they're up here, they couldn't be here with us today. This I don't want these just to be us talking over here. So, if you guys have any questions at any point You know, go ahead and interrupt us. I hope all of you guys have planned to go to the career fair, because you're basically one year away from graduating. So this is the perfect you know, the perfect moment for you guys to start looking either for one last internship and start to getting to know the recruiters because probably if I see you this year, and you come and give me a resume next year that you come and give me another resume I'm going to be like, "Oh, you know, I saw this guy last year he must be interested because he keeps on coming". So even if you don't get a job, it is good to go and stand up over there and going talk to recruiters and you know, submit your resume. How many of you guys are planning on having an internship? Don't be shy. Okay, very good. Very good. How many of you guys are currently working? That's the nice thing about UTEP, that most of our students actually have a second job and as a recruiter, you really appreciate that because you guys have already kind of have that culture of knowing what it is to do work in some people that, you know, sometimes when they do an internship, like the first time that they have work. And so, you know, don't think that that as a disadvantage actually, you know you were to say that. That way recruiters can say that you know how to work. So, yeah after graduating UTEP I was started working over there with the, with the army futures command and I have been working over there with the army futures command for three years. Some have gone to some places one has gone to many more places. But yeah, it is constant than it is a very fast paced environment. And that's why this tool is important because you don't want to be taking forever and doing a security assessment. And this tool is going to help us improve the time that we spend in writing the report and notifying the team lead. You know which vulnerabilities Have you found So that any further ado and before we do anything else you know I always take a selfie with the classes that I attached to so if you guys don't mind I'm going to take a selfie for the future. You guys ready?

So okay stop us if you have a question because basically the quality of the product that we are going to get and that you're going to work on, it depends on how well do you understand you know the requirements. And this is one of the most important phases of software development because if you don't have a solid understanding of the requirements, then probably you're thinking the product should look like this and your customer is going to think that the product should look something different, okay, you want those two visions to be one, and through the requirements we get to, to actually agree on what is it that we're going to work done. So even though it is not hands-on the keyboard, you know, programming the software, this is I believe the most important part of the whole the whole development process. Okay, so…

Speaker 11:18: Okay, so the department of defense, So every technology system that we purchased, right, has to be secure, must be resilient to attacks, must be tested and expected operational environment, right. So and here must be tested in expected operational environment. what is what does that mean? What do you think that means? Let's say you let's say you write an app, right? And you do all sorts of tests in your life. It's ready.
How did you test it? Oh, I thought about every single case that I could possibly imagine and I tested here. What happened just this week. No, the voting fraud and the caucus necessarily voting fraud. Yes, voting. Voting problems, right. What happened? They hired a company. company name is Shadow, you can read about it a little bit so you can see what happened, right? And before it was coming out, we could hear the chatter. And we can tell you weeks ago in the cyber security world saying, hey, so does anybody notice this? Because cyber security world at some point, it's very small. Yeah, you start seeing you start knowing who's who, right. Like, we just did it. So, I wonder what kind of test he ran. I wonder, you know, talking about some degree test, and then they said, was it ever tested in an operation environment? In other

words, if they ever go out and say, Hey, a school board in this high school or whatever, let's test this application. Let's have the 2000 students here. tested. We're going to mimic an operation of ours a real world or a representative life. That's what this bullet is right? So, that's very important. And obviously, that didn't happen because they had a lot of problems. And that's why I still don't know for one in either one, right? Okay. And it must go again, through many rounds of testing, right? Because you go to testing, you get all the results. And you're like, Okay, what happened here? How come right now, right? So, let's go with this outcome. One of the big problems is that people were not trained to use that, first of all, so they were having problems downloading it, logging into it. And then they were having problems submitting the results. So, there we had a training gap, right, we didn't train the individuals. And then the app itself was having problems and I'm not too sure exactly what was happening. They were having problems updating the results. The results were inconsistent, the way they were being they were being. So obviously, there was not a lot of testing. So they're very important in an operational environment. When we do test, we go to what they call developmental. So let’s say you’re writing an app for me, I'll come and you'll get an organization And we'll test it. And we'll say, Okay, let's run these tests. And then we see something wrong and then you try to fix it. And that's kind of like developmental, right? But now you say, Okay, I think it's ready for for beta, I'm going to put it out there. And I want to do a test in an intended environment. And I'm going to get similar users to the users and the operatives that are going to be using business.

Speaker 14:23 Then after that, you basically run through like in the field, like for example, let's say we're developing a radar system for a tank first you test, you know, your own company runs multiple tests, then they give it to the user in that kind of like a lab environment like he was saying, and then we test it over there and finally, we put that a you know that system on the field and then you go into that operational environment. So basically, all the tests that we do are happened through the through life of the technology right under development. So sometimes we will have meetings with the designers of systems before they like we're doing right now. And they consult with us, which will be the security requirements of the application or of the system that they're building. And then through the lifecycle of that technology, we go and assess because you know, as technology get old, or as you update technology, new vulnerabilities come up. So you have to, this is like a cycle, you know, things that you have to be learning…

Speaker 15:30: How many of you are doing cyber…?
Social viewings, even those of you that are not doing cyber, make sure to try and get just the basics of cyber, because at some point or another cyber cyber is going to touch you. Okay, whether it's development, whether it's testing whether whatever it is, and a lot of times when you're doing interviews and when you're trying to get a job, you want to get those little keywords that that is going to catch their their year. This is one of those words right here. Resilience..

Speaker 15:35: social viewings, even those of you that are not doing cyber, make sure to try and get just the basics of cyber, because at some point or another cyber cyber is going to touch you. Okay, whether it's development, whether it's testing whether whatever it is, and a lot of times when you're doing interviews and when you're trying to get a job, you want to get those little keywords that that is going to catch their their year. This is one of those words right here. resilience,

Speaker 16:01: Resilience means is enough

Speaker 16:05: Yes. Right. So it's it's try practice work down get into your mouth you know what you're talking about. So yes I want to

Speaker 16:15: develop software

Speaker 16:16 : that is resilience. Resilience is you know again whatever but look at look at the doesn't have to be cyber it's just it's just that those little words this is this is the government's using this a lot and industry single that we want we wanted they said oh we don't want to test it you have flaws. We're gonna test the resiliency of your system you know, what in the world does that mean right. But there there is there is something very special networks. So, we talked a little bit about what we do, right. In our particular army environment is we ensure survivability and lethality right, those are very hard work survivability. First of all means what? That in a contested environment. Our systems are Going to survive. And we're not talking about the cyber attacks, right? But we're talking about, hey, if they start shooting at us, our server is going to be safe. You know, speaking in our CS world, right, or engineering world, but that's where survivability means in we also do survivability of tanks. So we get tanks and start shooting at them, and then they will test Okay, what if these types of guns to to attempt to the tanks and stuff stuff like that and the second part is lethality. We're, we're more heavily involved in a defensive part, and also doing penetration test me in a defensive part means we're not the ones that are attacking or are doing operations against like other countries, right, Russia, Iran, but we do have groups within the army within the NSA within the CIA with FBI that they do the offensive part. So for us, some of the tools have to be legal. In other words, if we're going to launch a cyber attack on somebody that to better bebetter do what it's intended to. Okay? So we want to or TPK capable of being very lethal. And if we're going to go down, we're going to take our service or whatever we're going to whatever, that to better be that. Okay? And we're not talking only about software, but about everything

Speaker 18:23: We do per hour we perform a number of vulnerability assessments, and we'll talk a little bit more about this. When we start doing the question and answer. I think if you click one more, this turns into red, very cool. She was just kind of business.

Speaker 18:38: This is the cooperative pen testing. We do a lot of this, which is when we're talking about pen testing is we could be like this, let's say us, our customers, and we came to test your organization, and elseis your pm. She's your program manager. I'm sorry, your last name Elsa?

Elsa, we will call her your professor so she's your PM, she's your product manager. Okay? And we come in here and we'll say, Okay, guys, we're going to test your systems. You guys continue working the way you're working, you are going to be launching some attacks. If you see anything, let us know. So they're not selling, you're working out there and hey, my mouse froze. Or, hey, I see a pop up here that says to enter my password, or Hey, I see my password here says that I that a, a scam was detected. Okay, then we go to you and say, Okay, what did you do? Okay, so what we did is when you did, and then we start, we start communicating, okay, so that you can strengthen and make your system more resilient. Okay. All right. And then observe. This is this is another part that we do and suffer to actually is doing a little bit of this with one of the tools where we have served adversarial defender activity. Okay, so if you're doing the attacks, right, we're here doing The penetration test, we have another team doing the defense, they're using McAfee. There's a bunch of other tools, enterprise tools that are actually getting those things that you're seeing in your system. They're being aggregated.

Speaker 20:19: They're getting all the logs of everything happening on the network and on every independent system, and not say which one but in one event, we have 450 million locks. So imagine having to go through out those logs without any clue of what to look for. That's what they seem. That is just observing. The whole thing is trying to come up with the which ones are the logs that are actually giving you the story of where were you attack who attack you and from which systems which is the systems were compromised. So it's basically the analysis of how that amount of data

Speaker 21:00: So what is what is penetration testing, right? A test methodology which assessors the people that are testing typically working under specific constraints, it's usually what we call the, it's kind of like our like our requirements, or the rules of engagement, the ROI attempt to circumvent to go around right, or defeat the security features of an information system. So as a penetration test, right, if you go here, you can see and there's different models out there, but they're all you know, kind of like the same Sony was we have the pre engagement interactions, which means, okay, hey, I want to I want pent a pen test either because I want my system to be more secure or because I have this requirement from the federal government that says I must do cyber testing. And that's probably where you're going but a lot of you are going to end up working underneath your your piece of code is going to undergo cyber security reviews

Speaker 21:53: or it has to be compliant to different laws that are coming up and I don't know if you guys are aware of it. For example, of the health industry hospitals clinics have really, really heavy requirements on cyber security because we don't want that data to be stolen. Okay, so those require law, they have to protect their system. And those systems have to be resilient to X number of, you know, attacks. So, there is a huge contract right now going for police in which they're hiring a lot of computer science majors to go ahead and meet these requirements because by I don't remember exactly the exact date in 2021 of the health institutions have to comply with those and first are the federal institution. So what is one of the hospitals that have to meet this and then are the other commercial institutions related to help cover to meet those requirements? We're going to give a copy to students okay. So this is going to be a very, very interesting and very good, I guess, graphic that you can go back to the to the to the to the we need the week because we need help, we need Help organizing the way we do our work. Okay? Because a lot of times we end up being at the end of an engagement or at the end of the assessment and saying, how should we do this and who did that, and it's a big mess. So we need we need help solving that. We're pretty big group. We're about 80 in the army. And there's, there's more. There's 80 government employees, there's a lot of other contractors, and then there's the Air Force and Marines. Everybody has a soldier, let's say, I don't know. It's probably like 1000 cyber security analysts that do kind of this type of work in India. But where we started, it's kind of like right here, the pre engagement interactions, right? Hey, then you test. For whatever reason, either I have a requirement, or I just won't do it, but usually is because you gotta meet the requirements, right?

And they come to us and order on those requirements. For example, let's say we're going to test this tank that has a communication system. And then you go ahead and you don't want to be able to have I mean, let's say you hack a third party company and then through them you get to attack, that was not the, you know, the intent of the penetration testing, you want to, you have a specific system that will be under that under that test. So that's where you set up the rules, you're like, Okay, you cannot, you know, have at&t and then get through a radius. No, you know, I just want you to check the radius directly, if you can, you know, get into. So that's where you find out that.

Speaker 24:23: So yeah, I'm going to give you a quick example. And then we'll go through real quick. So we were hired to uh by the Navy, okay, by a third by a private company that was working for the Navy that developed a, a system where they could come and then kind of like, look at your iris and your face and your hand for all these biometrics, right. And it could be very quick. And I could see I'm gonna I was going to check those biometric results against a big database that I had to see you if you were on the terrorist watch list. Okay, so was this little handheld That the soldiers were going to have you were going to go in there. And it was it was like a little block, and then you were going to put it against your eyes. So scan your eyes, put your hand, look at your face, right? And then it will be right away. So we were higher there. So we started talking, and what is it exactly that what that you have? What is it that you need? So they send us the documents, right? And then we started doing some intelligence gathering, okay, then we go to our classified systems and say, Okay, what do we know about this? What do we know about the terrorists watches? Who keeps them? Where are they kept? How do how do people make it into that list? Who determines what? Okay. Has there been any cyber attacks against these types of systems? Or do we have information that they're trying to, I don't know, circumvent the way they do things. So we go here. Then after that, there's this other organization where a lot of spys come out of the DA in the in the engine, the National ground Intelligence Center, or the DIA, which is the Defense Intelligence Agency. And then we go there and they're like, okay, have you guys identified Any, any types of threats that you think could possibly affect this type of system? And so they come up with a report. So we got to read that report, right? Then after that, we're like, okay, we're going to go to Bahrain. What do we know about the area? Right? Where are we going to be staying? Who's going to be driving us around? What are the current threats out there? What areas can we go in and go to? Okay, so we don't we do all that. And then we finally go to this to this phase, which is a vulnerability analysis, we're out we're actually going to be sitting there in an operational environment, right with the operators and we're going to be testing the systems. This is where the two Frick comes in. Okay, we go there. By the time we get here, we already did the pre engagement interactions, intelligence around threat modeling. We already have a test plan. We already talked to them and they know what we're going to be doing. Dr. Perez is the lead in Frick. He's going to bring Frick, kind of pre populated because he already has an idea of all the threads that he's going to be Running, he has all the systems hopefully that we know of, right? When we get there, then we see reality right? Then we say, oh, shoot.

Speaker 27:07: Yeah. And that was that is most of like 99% of the time is different from what you have planned already. I mean, what you plan takes care of a 60 70% of the, you know, of the things that you think are going to happen over there, another 40% have to do over there on the fly. And unfortunately, when we go to these engagements with the systems, you don't have all the time in the world. Usually we have one week at most, two weeks to do that. So if you or any of your analyst get stuck on something that's like really valuable time that you start losing now, if if you have to stop because of x, y reason. Okay, so after you have this plan, you start going and analyzing the system to see how vulnerable it is. And we have many vulnerabilities that a system can have that we need to check. So let's say 150 200 for one person to do, it will be impossible. That's why they're there. It was a team of analysts. And then the lead starts said, when you when you go under that concept, you've had like 60% of those requirements of for that list of stuff that needs to happen. Another 40% gets populated over there once you're over there with the system. Right?

Speaker 28:19: Yeah. And and so now he goes in there. And he starts, he already had his pass on his mind on what he wanted to do, right. He knew the amount of systems and we usually have an idea based on the amount of systems, the types of technologies or how many people we need. And he had requested three personnel. So if there's four of us in Bahraini now doing it and we go and find out that it's twice as big that we thought, because all the virtual machines that were in those racks, the folks who hired us, didn't really know what those virtual machines they just saw. Well, I see three monitors

Speaker 28:53: and it's three computers.

Speaker 28:56: And it turns out that it was 200 computers or 300, right. So then we Go in there and now Now we got a scramble and now he's got a he's got a task. He's gonna say, okay, based on what I see this other tasks things that we need to do and this is who I'm going to assing them to okay? Because guess what the customer, Elsa, she's got another system that she wants us to test in six months that she wants to take advantage of this one week or two week assessment that we're here and she wants to make sure and let Dr Perez know what she wants the next six weeks the next in six months. So in other words, she's going to take him away, him being the lead. So a lot of the times where they're working as analysts by ourselves and the only thing that we have or that we need is you know, is usually is just a little piece of paper, of the things that have

Speaker 29:45: other asks that needs to be completed and

Speaker 29:48: this is what he told me and then we're probably won't see him sometimes we won't see him until one or two Sometimes he'll be there but depending right, so these are the types of challenges that we have. That we do now we we scan the system We do a lot we use a lot of automated tools, a lot of manual probing and system based on that, then we start saying, we see that system vulnerable here, we may have an attack already that so we can start exploiting or I know I know how to exploit, I don't know HTTP or I know how to use cane enable or you know, some other tools I know I got a password cracker that can do brute force and this and this web interface, you know, whatever it is, so we do the exploitation

Speaker 30:30 : or maybe on the exploitation you prove that the vulnerabilities that you found can actually be exploited basically, you are here you see how can you attack the system or here you actually attack the system as a proof that you know the system was vulnerable. Now this is this this stage is very critical because that's where you actually show the client that their system is not functioning properly security wise on X, Y or Z issues. So this is so important that, you know, to a client, their system always is perfect, right? So this is very important that you get the proof necessary to show them that, you know, the system is vulnerable in these in these stages. So, at this stage, we usually have to get either videos, pictures, screenshots, you know

Speaker 31:22: Artifacts and you probably saw that on the requirements, right? artifacts, what are the artifacts? Those are the artifacts, the proof, because that's very important. And I mentioned that right. You go and find and say, Okay, I've got this too'l that's telling me that it's vulnerable to this type of vulnerability. If we're not able to exploit it, right, I can't tell the customer, hey, spend a million dollars fixing that vulnerability if I can't exploit it, right. And now, if I'm able to exploit it, that just takes that vulnerability to a higher level. In other words, the impact and the criticality of that vulnerability, it just goes higher . So I at the end of the day, what the customer wants is, he knows he's gonna have some stuff wrong with it or identify, he wants to see, okay, I've got 30 things that we found one of the top 10 that I need to fix. So I'm going to tell them we want to say, over here, right, we want to be able to say, okay, we found 30 things, we were able to exploit 15 of them. The other 15 Okay. We were not able to exploit at this point in time. We don't know of any, any any tools techniques that we can use to exploit those. So concentrate on this 15 and out of those 15 this five are like a must. And then you've got another guy, another geeky guys are standing just kind of listening. Okay, that guy is the evaluator. He's not part of us. He's not part of the myself. He's somebody that the government's

Speaker 32:50: like the referee.

Speaker 32:52: And he's there listening. He's just there listening or she they're listening, and they're actually the ones that are going to put the report and say and tell the Congress, hey that system took over. Hey. I think we are going to delay it or gonna have the funding or give them more funding or whatever, they can fix it.

Speaker 33:09
Now, remember how we said that this process is cyclical right after after we finished with this engagement? Next year, I may not be the lead somebody else new to the program, maybe they lead and then he's going to be like, oh, what happened? which were the vulnerabilities that we found last year? Which ones were exploited? How did they exploit it? And if they change the team and put somebody new out that information is just on a report, right? We don't want that that's why this free tool is so important because he will be able to allow us to kind of map the history of what happened at that event.

Speaker 33:51
And so you can freakin live in the whole thing, but mainly it's going to be around here. Around here.

Speaker 33:58
From here to the reporting.

Speaker 1 34:00
And as far as that, and I know probably as we probably going to choose some of the questions that that we're going to be touching, but usually the the assessments, these types of assessments are usually most of them are just five days long. Some of them are 10 days long, and I'm talking about the actual analysis and exploitation, okay, when break would be used the most would be those five or 10 days that were out there, okay? The whole, this whole process can take anywhere from three months to six months. Okay, from the time that we get the first interactions, all the meetings and then we write a test plan, then we send it to you, then you say, Well, I don't know what this means, or what about testing this. And so we do roots and the engagement and all that stuff. And then post exploitation once we exploit them, and we get all the artifacts and we get everything right, then we got to report. So usually what happens is let's, let's take the example we're going to go with the example of the five days, okay, we do the five days, we do about four and a half days of actual mobility says analysis and expectation. And then at the end of the fifth day, we we have what is called an ER-B, which is an (emerging results brief). Okay. And a brief is basically a report, it's just a fancy word for usually government that that uses that right? So we wouldn't call this a presentation, we would call this a brief. And I'm not presenting, but I'm briefing. Briefing right were were briefing. So um here, the very first product that comes out of that, for the lead is and that, you know, after those after everybody's taking the task. They're working on them. They find the vulnerabilities, they put all the information. The description, they get all the artifacts and what not and and the statuses and all that. At the end, I need to get a brief or umm it could be you the way we usually end up doing and we do it by hand is we get an Excel spreadsheet, right, but a certain number of columns, like for example, the vulnerability and type. The the IPS that are affected or the systems that are affected. That the impact of the vulnerability that likelihood and we will go into that a little bit later. But anyways, this is a report or a presentation that we give the land the last day on that fifth day. And we get up there and we say, Okay, this what we found, okay, and that comes to come directly out of this tool.

Speaker 36:24
This is so time consuming that since you have to do it on the same week, it is hard for that brief to contain a lot. That's why the tool that you guys are building the repository that you guys are building, to also

focus on that last stage, which is the reporting of what you found, and of the steps that took place for that to validate that vulnerability and this list of vulnerabilities that were found

Speaker 36:49
Cause how it works out right, let's say you guys are my assessment team, I'll go, what is your name?

Speaker 36:54
Jose

Speaker 36:55
Jose, hey Jose so umm what do you have to report and this is like Wednesday or Thursday. Because I got to do the, report and I'm the lead right? And then he tells oh well I found this this and that. And I just kind of write it down. And then I got to go type it up, right? And then come back. And so now you're, hey man what's your name

Speaker 37:12
Miguel

Speaker 37:14
Miguel. And Miguel will say hey man I got to talk to show you something. Hold on wait, I got to do I got to get ready for the ER-B and he like I need, hold on then. And then I come here and say what is it that you do, what happened to that second thing. What was your name?

Speaker 37:27
Jaime

Speaker 37:30
Jaime and I'll get. Jaime is like, Oh, well let me show you. Hey so do you see a so I'm here I'm there. He wants me over there. And then Elsa's over there. And Lisa Hey, can you give me a status? My boss that wants to meet with you for an hour. Okay, and I'm here trying to so then at this point, I'm like, you know what? Dude umm I'm sorry. I got to go be with her. You know what, hey, go and meet with them. Get all the stuff and do a brief for me. So now we lost this guy, right? And he's like, but you gave me all these all stats? Right that I had. I said, Yeah. If we have time, we'll do him. But if not, we'll just we'll just keep okay. So this is what happens, right? This is what happens. So I already took time from all of you just just by the interactions. Okay? What was it again? So how did you do that again? Right? And I'm writing things down. And I'm like, Okay, let me SSH into your box. So I'll SSH them to your box. And I'll try to look through the slots to try to understand, but I'm trying to reinvent the wheel, right? Whereas if we have this system, where you guys are reporting, and you know what you guys need to report, I can attend to it. And then at the end, I can just come after us as we in common and look at my box and say, Okay, I see what everybody's done. I see where everybody's at, I see what we still need to do. And by the way, let me export or print this ER-B this table that I'm going to put on my brief, right so that I can present. So

This is just, again, it's that same one and as we as we talk as you meet more with with Arandi and Vince and ourselves and whoever comes, we're going to be talking a little bit a little bit more about this. But if you notice, all these seven this year, or plates or bullets, whatever you want to call them. This is the scanning and enumeration of targets. So it's again, it's it's identifying

Speaker 39:20 What happens with those expectations that you didn't find an answer. And um you know how you said you had 15 and 5 of them you did find an exploitation and 10 of them you know are vulnerabilities, but you haven't found anything. What happened to those?

Speaker 39:34 So we still report them. But those get those get classified based on on so let's say, let's take one of the first five, those are the easy ones, right? Because we're like, okay, we were able what were we be able to. Okay, I exploit it. Okay and so what? Okay, why did number one give me? Well, number one, gives me access to your web server and I can take your web server down. Okay, that's got a possibly a high technical impact right? Like, okay, because you're taking the web server, okay? And then so what, who needs that web server, oh well that server is something that we use internally, so that people can tell us when they went to lunch. And you're like. So now you can see that the impact to the mission. It's not probably not primary not, because the mission of that service was to see if Russia was about to shoot a missile or something right, telling me when you're going to go lunch may not be a so even though that one meal, you got it and you took down the whole server, whatever, maybe that it's a high technical impact, but the mission, impact is very low. So then we rate each of these vulnerabilities. Now. So that's, let's say the second one is okay, I was able to break that system. And now I got a root account to your system. And by the way your system is is is a is trusted by the domain controller. Because that's the system of one managers or whatever, and I got into the domain controller got everybody's passwords, everybody's whatever. And now I can really mess with all the integrity of the information. Now the impact, the impact the site, and the operational impact, or the mission in that is very high. So now that vulnerability is a high, so when I reported it on that frequently comes out, that second vulnerability is going to be a high, the first one is probably going to be a medium low or a low, low mission impact. Does that make sense? And we'll talk a little bit. Now the other 10 even though we were not able to exploit it, we still have to say, okay, you know, what, these 10 these first five, you know, we don't know, even if they were exploiting it, what if even if there was something out there, we're going to go through the same drill, right? Even if there was something out there that could exploit them. Now I enter the so what, these don't have very high mission this particular this 11th one, if somebody is able to ever come up with a way to exploit it, it's game over. So we're probably going to bubble that one up, not too high, because we're not able to exploit it now but maybe to a medium, just so that it's out there, and we're going to type it as, hey, if once you fix this 5 lets, let’s get this other one but but it’s going to be scoring

Speaker 42:12 So they still go into the report but, you know, they haven't been validated. Like they said over here. Okay? That's very important sometimes. You know if that gets buried into our report next year that we come and do that assessment we are going to be like ahh, you know which ones we couldn't validate, and then you go, and then you validate the ones that you did last year, and then you're like, Oh, I wish we would have had that list of the ones that we didn't validate. So we could just focus on those. So that's where your tool is very important, because you know, that is going to leave over there on that on that system. You're going to say like, Oh, these ones were exploited, and were validated as, you know, actual vulnerabilities of the systems in these 10 you leave out so next year, when we go we open the software. We're like, Oh, look, this is the map of what we did last year or this one. We're missing, we still need to do, you know, let's not focus on those based on the priority or the visual impact, or the technical input

Speaker 43:08 And um this reporting will probably update a little bit this a little bit. But as soon as we start here this 5 day the engagement in most of the engagements or most of the tests, we have a brief presentation everyday. Yes, Elsa has her boss telling her Hey, okay, Mondays did we find anything? Yeah. Are there any has anything burning? Do I need to bring the folks from New York like Wednesday he's on standby to come and fix it. So by the end of the day, as the lead, right, he needs to go in there and see if there has if there's any burning issues right now, because at the end of day, she's going to have what we have called the Daily hot wash.

Speaker 43:49 And really quick this is so important to the to the organization's because, and I'm just going to give you an example once we were analyzing your system that I believe their budget was over 100 million dollars. So they want to know, and they want if you find something very critical, they want by that by the end of your engagement, they have fixed it, because they have you over there for that week. So basically, they're like, Oh, you found something that is really, really critical. If you let us know, on Monday, we'll bring the team of 20-30 engineers over here to the field to fix it on this system, so we can replicate the fix across the whole, you know, system. So real time communication among the analyst, and from the analyst to the PM is really important, because, you know, that's when when they can fix stuff like right there on the like on the Operational Test, which is very valuable for them and it will be very valuable for us to keep track of all this issue.

Speaker 44:49 Yeah. And then the last thing just last year, last one right here is on the reporting. So we have that ER-B that the emergent results brief, two weeks after that. We give them a risk Assessment. So it's basically that ER-B plus now we go in, we assess risk right in there in the ER-B, we gave it a quick, like he was asking um, high, medium, low grade, if you may, for each vulnerability, two weeks from there, we sit down as a team, right during those two weeks, and we go through each one. And even though we can rate it number one is a high this case as well, because he has more experienced in that particular Window System. He says, well, but you know, if you do do that, then you have all these protection mechanisms that are going to be protected. So even if you do that, and you take care of that whole thing, look at all these things, all these things are going to mitigate it. So I would say it's not a high high, I would say it's more like a medium, because even though it's going to affect the whole mission, it's going to be game over. There's no way you can do anything of that because all these protection mechanisms are going to take you down right away. And you're like, Okay, so now you give value to the protection mechanism that are there. So even though it's very high impact and relevant to the mission, you have already a mitigation within your system, they can do it. And so we that's what we give, we give a risk assessment. Okay, now, that's about that's about two weeks after that now 30, business days, 30 to 45 business days after that after the the end of the assessment, which will be about another three weeks, then we give them a full report. And that full report, it has like four main sections, right, like the introduction, the system categorization, not that system categorization. The system description. And then we have like the results in discussions, right, so we put all the results and the findings and the mitigation strategies. And then we have the conclusions, which is again, what do we recommend right and in there?

Speaker 46:49 Yeah, and really quick, when we're writing these reports, you know, a month after the event, sometimes you're like, and like right now you have your notes and you're like, oh, man, I don't even understand my handwriting. What was I doing over here? How did I, how did I exploit? How did I exploited this vulnerability? Ahh did I do this? Or did I do that. That's why this this tool is so important because thanks to this tool will be able to document these either with videos or with screenshots and of course we text but you know an image is worth a thousand words so we want it we want the system to be able to capture all these screenshots so that we can then go back and say like oh no, look actually let me see this this small video that I recorded on how I exploited this vulnerability. Oh I want here here and here that way when are you writing your report you can be more specific because the customer values whenever you are specific. Can you tell them how you were able to do you know that exploitation because now they can go back and fix it.

Speaker 47:51 You know, I told you how how Elsa was taking our lead right to go brief and everything so he already missed some things that went on during the during the week or whatever. And guess What? Now? When we're reading the report, the three that were on his team, they got called to another assessment. So they're not available

Speaker 48:06 OK so you guys are gone and I'm like, Oh, how, he told me that he wanted to talk to me. I don't know why I don't know what he was doing.

Speaker 47:51 You know, I told you how Elsa was taking our lead right to go brief and everything so he already missed some things that went on during the during the week or whatever. And guess What? Now, when we're writing the report, the three that were his team, they got called to another

Speaker 48:04 assessment. So they're not available, you guys are gone and I'm like, Oh, hell, he told me that he wanted to talk to me. I don't know why I don't know what he was doing.

Speaker 48:13 And so what we do now is, guess what we do, I get his drive, I've got Miguel's drive, I've got Jaime's drive, and I've got Jose's drive. And I got one computer. And what I do is I take my drive out, I give his drive in, and I try to understand what he did. Yeah. Okay. And it gets pretty hard because I like to do it a certain way. Even though we have a directory structure sometimes like my little sandbox, right? I have a little directory that I don't share with everybody, because that's where I put my notes and that's where I keep track of my stuff. I don't know what he does. So I go in there and like, I guess he didn't do much because I really can't find anything. Right? And that's why if I had if I had this tool that I could just go off to the point that had been syncing, you know, I don't know, every hour or every, you know, twice a day or We're on a push up button or whatever, or all of the above. I could do that in a daily watch, and then I could say, Hey, you know what? My boss, his kid, has a soccer game today at five. And so we're gonna have to move the four o'clock meeting to two o'clock, because that happens. And then like, oh, shoot, I'm not ready. And it's one o'clock already. And we got to drive 30 minutes to whatever. So now I can go in there. And I'm like, hey Jose, and Jose's like, so Jose is so engaged. He doesn't want to talk to anybody. Right? Because he wants to, he wants to make sure that this, this is central by the way, he works with us also. And Jose he doesn't want to talk to anybody because, he's like "hold on, hold on" I'm really close to explaining this. So I want to have this ability to say okay, sync with Jose. And I'm this thing's gonna reach out. And I'm going to get the latest like I want to get the latest and I'm going to sync with everybody, right? And then I want to be able to cut or I want to be able to export either to an Excel or PowerPoint or doc whatever or PDF. Whatever it is, or all of the above, I don't know. And I'm going to be okay. So I'm ready.

Speaker 50:05 Maybe a web Interface that says these are Jose's notes, these are Jose's screenshots, screenshots, these are Jose's … yeah

Speaker 50:12 you know what everybody, it's going to be that that format and now I can go, Okay, I'm ready to go over there. And I can go and connect. And now we can start presenting. Right? I can start briefing

Speaker 50:22 So basically only the lead would be able to do that

Speaker 50:25 or

Speaker 50:25 No so. So both really good question. Very, very good question. And, and the syncing would be both. So there's, there's going to be a lot of inherent trust between this because it could be Tuesday, and I get sick. Or it could be Tuesday, and outside just happened. You know what, we're gonna go two days to this other thing, whatever. And I'm just gonna leave my box here. So you guys have to have the ability as analysts to sync both ways.

Speaker 50:55 Like you were saying, let's say you get pulled by the PM and then suddenly somebody says no You're saying, Hey, can you brief me on what has been going on and you have, you can say like, Oh, this is what I was doing, you know, but I don't know what the rest of the team was doing. We don't want that to happen. We want him to be able to say Oh yeah look, I'm doing X, Y, and Z, Jose’s doing X, Y and Z and you're doing X, Y and Z.

Speaker 51:15 Yeah. And then we've got what’s your name sir? Chris We've got Chris here, who's like, he's super organized, super on the ball. Every hour. He wants to tell me he wants me to know exactly where he's at and what he's working on. He hasn't really exploited anything, but he wants me to know where he's at and what he's working on. Okay, we've got over here, Christian, Christian, Chris,

Speaker 51:40 Chris, Chris, too. We've got Chris

Speaker 51:42 over here, who's like me, he's like, kind of scatterbrained and kind of like, and he's like, gosh, I'm not gonna report anything until I find something and everything's fine. I'm not going to give him any piecemeal. I'm going to wait until the end of day. Okay, so when I go there, I'm going to have Chris's notes but I'm not gonna have his because He already went ahead is in synced with me, right? He's been sinking. He's been updating with him. He doesn't want to do it. Right. But he's got hi stuff but I'm going to go ahead and sink his stuff to me. Does that make sense? So it's, it's, it's got to be it's got to go closer So you’re saying like, even if I don't, I don't want you to see my stuff, you can sync it? Well, if you don't, if you don't want me to see your stuff, I’m still the lead, right? I can still SSH into your box. And you can SSH into my box, because that means there's this trusting, right? If you don't want me to see what you're doing, then you're not going to update your Fric, or this tool, right? You're going to have everything else out there. But if one o'clock comes, I'm going to say hey, you know what, where are you ? He’s like, you know, I haven't finished, I have nothing to report. And that's fine. And I can just and then I can just say well, what are you working on? I'm working on this. This is going to do XY and Z. And I'll be like, Hey, Chris, can you just split the task? It's task three, right? You're working on task three. Okay, at least I'm going to say now I can go at least say at least say, I guess at a minimum. That's a… That's a good point. And I'm kind of thinking out loud here. And a minimum, what I want to see is that you're working on task three. So I want to be able to sync. I can’t see what you've done the results or anything because you don't have anything, but I want to see that at least okay, but he's working on task three, and he's touched sub task three and four. Those are, those are in the works. It's kind of like a ticketing system. And there we need help. We don't know. We don't know if if it's a percentage. Even though we've said I think on the on the description on the requirements, I think that we want a percentage or a numbering or if we just want something that says ending or being worked at or I don't know, we need help with that. So see if you can do some research on a like ticketing systems and updates and those and then see if you can recommend something because there we all think a little bit a little bit different.

Speaker 53:51 But we want that for example, let's say you put stuff on fric you don't have time to sync we want the lead to be able to say okay, you know, I want to pull the information from the his freak. You know,

Speaker 54:03 make sure you're taking good notes, especially the leads or, or the representatives the represents that group. Because what we're talking right now, okay? We're kind of agreement stuff, right? And believe it or not, next week, we're not gonna remember what we agreed on. And then we're going to come and say, well know what I want this 25% 50% 75% 100%. Okay, so take good notes, and then you're going to report it to your professor. And then she's going to send them say, Okay, this is what we agreed on, right? Or this is, this is this is what we understood, and then we can come back and say, Well, yes, no, or Yes, exactly. Okay. And that's going to be this is going to be modifying or, or putting those rules of engagement or those final requirements.

Speaker 54:54 As you mentioned, in the future as our developers, this is very important these back and forth between you and the client. always always exist. Okay. And you have to be able to put it in into a written format like elsa does that way, both parties can say like, Oh, this is what came out of the requirements meeting. This was our understanding, is that is that synced with with your understanding?

Speaker 55:17 Elsa, It's at 10:50. Right. So we've got 22 minutes. Okay, so we got a few more slides, but hopefully we're answering some of the questions right now. And I want to have a good 20 minutes so that we can just go, you know, straight with your questions. So, let's see. I think this one… I think we can we kind of talk

Speaker 55:37 a little bit about this, and we're going to give you a copy of this presentation. Okay. So,

Speaker 55:42 okay, this is this is the the actual tool, right, the shoot suit, facilitating collaboration for for individual tasks and findings. Right. So those are two main things right tasks for I know what I need to do as an analyst and what we think need to be done, and then the findings right, the way I went to report it back, right? All of that, again, there's a lot of trust between anybody, everybody. Hopefully there's one leak or one server maybe I don't know. And then also, what is your name sir? Joe? Joe and Ben, Ben, Joe and Ben over here, right? They're very good at threats. They know threat up and down. Dave has so much experience that when we go to that engagement,

Speaker 56:27 Ben, Joe,

Speaker 56:29 Joe and Ben, Joe, Joe, Chris, Chris, and,

Speaker 56:33 Ben, Jaime

Speaker 56:38 Okay. And they're very good at that. And we know that we always know that when they're on the events, these guys are going to come up with more tasks. Okay, because they're going to see the world different. They're gonna be like, Oh, yeah, let's see what Miguel did and what Jose did. And we put those two together, right? We can come up with this, combine the tech of this. So let's do This task and it's assignment to Jose, or let's assign it to myself, or let's put it on one of those, it would be nice to do. But if we don't have time, we're not going to do them. Okay? But we're going to do tasks, okay, so So for these tasks and the sub task, we can, again, it's got to be, we got to be able to have that communication. And you guys have to be able to also

Speaker 57:20 create new tasks

Speaker 57:22 in the ability to create task really quick. Let's say I'm the lead and I already had the task for my analyst, right things that I have assigned for them to do. Let's say you find something else, and you're like, Oh, you know, I'm focused on this on this. I don't know this vulnerability, but I found by looking at this, I found another three things that could be potential, potentially vulnerable things. So you should be able to add that to the task list, kind oh, for tomorrow, I want to focus on this and this and this. Okay, so that you can add to the analysts can also add to the task list that needs to be done. Because of the stuff that they have discovered

Speaker 58:02 is there a basic structure of tasks that have to happen? Like on each task? So for example, you know, you have to create tasks for ...

Speaker 58:11 Yeah, but bottom line Yeah, that there's a, there's a, there's specific tasks that we have to do. We do have a procedure whenever we would, that we follow whenever we do. Like, for instance, the tvpa, which is one of the tests that we actually performed was about 70% of the time. So like, for instance, a procedure will say, hey, you need a you need a scan the network with within that, once you do that, then you have to scan the network with NASA's once you do once you do NASA's, then you're going to run this tool called kudy cannon. So essentially, essentially, this tool is like an in house tool that we developed that it's going to take the results from NASA's is going to go out into the network and pull down snapshots from from the different systems that are out there. And then after that, you're going to say oh, well I want to do this I'm gonna start doing the traffic analysis parts of a, someone needs to run Wireshark someone needs to analyze what the what's on Wireshark after that, oh, let's, let's see, we want to poison the we want to poison the network. So hey, someone's gonna go in and we're gonna, we're gonna do like, etherool, is that the tool?, so it's better cap ettercap bringing out we're going to run an ad recap, we're going to poison the network and we're going to see what else what other information we can get. So I mean, we do have a procedure out , i dont know, is that something ...

Speaker 59:32 usually the lead will have that pre populated list, remember that 60% that you you've come into the event already planned? Usually is that what Michael is talking about those tasks

Speaker 59:44 in those changes? Like right now what right now we do have a minimum stuff like you said that we're gonna go do but that changes through time. Yeah, so right now

Speaker 59:57 And so the different events so that can be That should be kind of like I guess customizable for an event, but it could allow to say, Hey, I have this this fric version. And by the way, when you start up the system and you start a new project or whatever it is, I have this set things that we will have to tell you a template. That would be that would be awesome.

Speaker 1:00:21 So far with like, basically like a finding of finding can get into like a new task.

Speaker 1:00:27 It could, it couls. Yes.

Speaker 1:00:29 Let me see if I can, can we think of something really quick? So let's say I found the

Speaker 1:00:39 we think that the domain controller let's says I found that domain controllers uses default credentials, and I was not expecting that. Okay. And so now I have access to the domain controller like oh shit. Guys. I have I have access to the main controls. What do we do now? And they're like hey and then this guy's like, right ways the things that you want, hey, pull out the mtts that did The password they hide. And let's get let's let's let's see if we can crack any passwords of other systems or other domain controllers. So we put that task and we're gonna assign it to a drop whatever you're doing, because now this has higher priority and work on this first. Okay, and so it'll, it'll start new tasks. And then and then hey he comes back 20 minutes later, Hey, I cracked the three passwords for the domain controllers on the sea, and we have access now to whatever, well shoot. So then all the other tasks that we were trying to do to try and break into it, now we can break into it. So now there's gonna be some tasks that are made the primary, they dropped from priority? Because we already have access to that. So yeah, so that's going to give us we're going to create new tasks, and there may be some tasks that we're going to that we're just going to close

Speaker 1:01:49 So like if you still want to keep track of that, finding that created the new task.

Speaker 1:01:55 Yes. Okay. Yes. In fact that that might be that might be in fact, that might be a subtask Let me tell you why that's important because when we're reporting, we're going to say some people say, Oh yeah, I was able to get into domain controller and I cracked all the passwords and yeah, we were were we own your system when when the task was Hey get without stuff and ask her to give you the passwords to get into a domain controller so that we can assess the system so she gave me the password and everything because that was my test. Right? But the way I presented it to everybody and to reality there was a yeah we got in there and we got him for No, we could have never gotten in there tasks we had all these other little sub tasks and we found these these but this is but but she opened the door for for us

Speaker 1:02:48 to know like the main tasks

Speaker 1:02:50 yet then what came out of the flow. These are all the task in the project, right? like Like, there's like this. There's the system like you guys were analyzing Inside this system, are all these tasks that like that to do that, yes. Like all the tasks to the finding, right?

Speaker 1:03:08 Yes, that have. Okay, so you start with this guy, right. So this is kind of like that first prevent. And what's more likely is, hey, we've got these 10 tools, we need everybody, you're going to be assigned these 10 machines are going to be assigned this 10 machines, you're going to be assigned those 10 machines, and you're going to be assigned those 15 machines. And I want you to run with all these tools. Okay, and those machines, so that's your first task. So boom, you go, you get all you gather all the information, right? And, and then you're updating where you're at and everything, we're still not doing any findings. And then after you do all that you're going to analyze your results. That's going to be another tasl, right? So okay, once you finish all this, I'm going to analyze the results. Once you analyze the results, right, then you might have subtasks because now you say, based on based on what I see here of the information that I've gathered, I've seen that I have 10 different things that I could possibly explain. So those may be full tasks or they may be sub task of what I found, right. And then and then you go and check one you're like app, it was a false positive, because they've got this and you got Oh shoot, I was able to get in or you know what the system got in because a lot of times the tools will also try to exploit you like I gotta find in here, default credentials and a web server. And so that's a finding. And here's my, here's my snapshot. This is I'm going to put a little video of of just I found the website that I got in there and I'm going to pick any of those things and I just want to show what it's there and why it's important. Oh, look, this one is all the social security stuff everybody that works here. This one Oh, look, this is the managers whatever and he's this one he keeps track of everybody's username and passwords

Speaker 1:04:49 Are analysts working in more than one system, like analyzing system or are they just working

Speaker 1:04:57 They their main computer but they work Analyzing several systems

Speaker 1:05:03: Yeah. Okay, so so let's say, let's say that we were in this could be up, let's say we're all analysts here, okay, you're going to shop with your computer, all your tools on your computer, you're going to connect to a main switch, right? And I'm going to, okay, you're going to be 10.0.0.1, you're going to be 10.0.0.2 and you're going to be 10.0.0.3, that's going to be our collaboration, that's going to be for free, there's going to be updating to us, and they're going to say, oh, and in the system, because you're gonna have to IPS you're gonna have to, you're gonna have 2 network cards to remain. And then on the second network card, you're going to be connected to the system, you say on the system, you're going to be 168.3.2.1. And that's because, you know, because Elsa tracking those because they're going to be watching, right, so you will connect, and then in the task, we have 300 computers and I assign you 25 and I assign 25 I assign 25 and I assign you 100 and hundred or whatever. And that's just for the initial part right for the initial part. Now, some assessments like the one that are pursuing a new assessment right now this week I asked them for today, they say just concentrate those 25 consonantal 25. And so that lead wants you just spend those 25, okay, and do all the tasks on those 25 and try to exploit anything there. And either most of the assessments is after we collect all the data right now, because we don't have a good, you know, organizational structure, it's a free for all. You just are like, Okay, guys, we've got other data, go at it. And that's what we do. And so what happens is, you're very good at windows, you're very good at Linux. You're very good at Mac. You're also very good at Linux. And you're also very good at windows. So then now I have these two guys who see these two low hanging fruit and they're like, Oh, I can exploit it. It's gonna take me about four or five hours. And then you go tackle the problem. And you're going at it together. And sorry, you guys and then five hours, y'all come on, I got it. Oh, I got it too. Oh, you guys work in the same thing. Oh shoot, maybe that one that was just wasted

Speaker 1:07:03: Five hours of an analyst working on something which could have another task

Speaker 1:07:07: Right or where we could have said, You know what? Let's tackle it together. Let's work together. And we might be able to reduce the time, two hours, because we're going to be working together, or, you know, so those are some of the challenges that we have. And depending on the leaf, like I said, some leads will want to just do sectionalize it, other leads are going to just do like a free for all. But Frank is going to allow us, it's going to allow the lead to do either of those. I mean, he could say, you know what, guys, we've got this 30 tasks this leads that are not gonna want to assign the tasks to anybody.

Speaker 1:07:46: They want to see the task and say like, Oh, actually, I want to pick this or pick that or pick that. Yeah, then task list. On the break, you should be able to say like, Oh, I want to work. I'm working on task number three.

Speaker 1:07:57: Yeah. And because there's a lot of times, a lot of time I'm gonna assign you 10 tasks that are windows and you hate windows, and you don't want to see windows and you know nothing about Windows. And then you know, same with the Linux. So, so again, it's its if we don't know each other, whatever we want to be able to either have them leave going there and assign tasks or some of the tasks. And then the other tasks, like you said, right, hey, we've got these 30 tasks. This guy finished all of his information gathering right away, this guy took a little bit longer and he'll just say, Okay, you know what I've learned? You know what, I want to take this one? To make you assign to yourself, okay, because I know I can help you with this one.

Speaker 1:08:39: I like a ticketing system, kinda like you know, there are these issues, who wants to take him or you want also the other approach in which Juan can say like, Oh, you take task one, you take task 2 , you take task 3. So when the system plateau, something better

Unknown speaker 1:08:53: So we've designed themselves a tasks to subtasks now can the leads create there own subtasks without analysts other than then the lead create there own sub tasks whenever they can

Speaker 1:09:08: Yes, yes. Yeah, because sometimes you get something task, you know, you get a task. And then suddenly you're like, oh, by doing this, I discovered that I need to now do these other four things, we want the analyst to be able to put those four things on the, you know, on the queue. So, if you don't finish what you're doing, but somebody else see that, see, I can see that you added subtasks so they can help you work on those subtasks

Speaker 1:09:34: And what we do. And so now you created some new tasks, right? So depending on how we we can, we can maybe put the system to every scene by itself every one hour or whatever, every time or by what we think it's going to be a two way scene, right? I'm going to go and I'm going to sync, if I if I say sync. I'm going to sync all your information, but then you're also going to be updated on the progress and everybody,

Speaker 1:10:01: like a push of your information and I do a pull of my information to you too.

Speaker 1:10:05: So that you all see, you know what's going on

Speaker 1:10:09: technically, like Juan was saying we always have four analysts computer connected to same switch. So you guys should be always on the same sub network so that we technically your computers are always connected to each other.

Speaker 1:10:23: Yes, okay. You mentioned that at the beginning, the analyst can see the other findings of the other analyst findings. And something that you also mentioned it was that there is a cases that two analysts are working together, can work together and refine it. So my question is, you also will want that for example, when I see for example I see you working in something I can

Speaker 1:11:05: You mean like assigning 1 task to two analyst?

speaker 1:11:08: No, I mean, for example, I can see that the one analysis is working in the past. And I am as analysis, I can collaborate with him. I mean, when you say,

Speaker 1:11:21: yeah, you can add yourself to that task Yeah, yeah, yeah, we want to be able to, to see that 2 analyst are working on one task. Or you as an analyst, you can say like, Oh, you know, he's working on the same thing as I am. Let me add myself to that task. Okay. So it is, it is seen by the system that two of you are working on the same thing, I'll say, yeah, and,

Speaker 1:11:41: yeah, that's, that's, that's it? That's a good question. And so yes, that would be the flexibility. Now, it doesn't have to be like in programming for like in the rational two, three, or whatever, you know, for you check out you know, piece of code and nobody can touch it. Not necessarily like that. Okay. So we don't want to we don't want to lock it.

Speaker 1:12:00: Yeah, we don't want to lock you

Speaker 1:12:01: But yes, you can. You can add yourself and that would be good. Maybe Maybe I don't know, I'm just kind of maybe a, ben over here says, Okay, I'm working on this task. Right? And when I see it, I'm like oh Ben's working on it, but then you have the ability to also say, you know what, Im going to collaborate with ben. And so at least at least we know that there's a little verbal and say, Hey, you know what, I think I can add to this, hey ben can I look at it also. Right? And then you collaborate. We're usually call located within walking distance, or we are seeing each other so that we can talk about that right. But yeah, that would be good that way. because let me tell you why that's important. When we're doing the reporting part, and nobody's here, right? I didn't know that you two work on it. That is an end. When I look at this sentence. It says, Yeah, I was able to done say Okay, what else did you know, like now, I can now talk to one of you two.

speaker 1:12:55: You are the lead whenever you're doing the report, you want to be able to go and see the findings the screenshots the videos the the you know the text of what them two those two analysts that you know wrote or or have over there very good questions guys. Yes.

Speaker 1:13:12: Earlier use system for for an example but how do you define a system in this case?

Speaker 1:13:18: This case you mean a system that I'm analyzing or my own system. By my own system is the laptop that I have with me that I will be connected to the other analyst and now system that I'm analyzing that's whenever Juan tells me Oh, you get to test this tank and that you angel you get you get to test this helicopter. So those are the systems that tank and the helicopter where the systems that we were testing .okay.

speaker 1:13:43: So systems, some kind of hardware, some kind of physical thing

Speaker 1:13:46: hardware or software

Speaker 1:13:47: Yeah, so, so, system is usually King you can see it as a as an IT system like essentially your laptops, computers, it could system can also be referred to as a system under test could be the entire tank itself. That could be the radius of the interrupter. Exactly. networking devices, suite. And anything that I guess, maybe it's something we should have cleared up. But a system for us is anything that we can possibly test. It could be a web at web application. machine. Yeah. Virtual Machine. It doesn't have to be physical hardware.

Speaker 1:14:24: Yeah. So let's say just to give an example of three, let's say, we come to this room, and, and one week we're like, Okay, what we're gonna do is we're going to assess the all the computer here, we want to see we can get into this that we can break into this computer from the outside. Okay, and so my system, right, it's going to be all the laptops that are here, and they're, they're out facing ports and whatever, whatever their their whatever they're communicating outside, right. And we're going to say, okay, that projector that's off limits, that's not part of the system, even though it's here. The switch that you guys are connected to and the wifi, that's not part of the system. Another test could be, okay, we're going to come in here and we're going to assess the Wi Fi. So your systems are your individual computer or system, they're off. So the system there, the system under set test, that's called a sub system under test, that's something very, very common is we're going to have boundaries, right? And that system, it's just going to be the wireless and the wireless communications between this between your computers and that access point. Oh, that's all we're testing. The third one could be okay, we're gonna were gonna assess Microsoft products. So we need to be able to get into your computers now. We need your passwords and usernames and passwords so we can get into your computers and we're gonna assess all the system on the test is only word and excel one

Speaker 1:15:44: only the applications not the computer itself

Speaker 1:15:46: right and we bind it right and even though I go in there and I see that your password is admin, or your your username is admin and your password 123456 and I see that's that's very weak, but thats not a part of this assessment, I can point it out to you say, you know, but that's not a finding. Because the only findings are going to be the system under test, which is going to be in this case, we're just going to throw in their Word and Excel sometimes.

Speaker 1:16:13: In the penetration test, that's like the first thing you do, right? You set the limit, you'll be what I

Speaker 1:16:19 : remember the the pre engagement back and forth, and the test one?

Speaker 1:16:23: yeah, that's this right here.

Speaker 1:16:26: You come up with one that I signed, and you signed, we were like, Okay, what is my boundary? Okay? Sometimes they go and say, hey, I've got these 20 systems. But I know this is very vulnerable. But I use this to this is this is the one that we use for everybody clocking when they get in here. And so right now well its not ready. So then they talked to the evaluator, and they're like, okay, we're going to put this other system, it's out of scope, even though it's its part of the system or usually for this test, that's going to be out of the Oregon test. I'm going to get a waiver because I have a plan for that. I'm going to replace this by a new system. My new computer thats coming in. So a system can computer many computers, but you just got to define it, you got to give it balance. Okay? Because if you don't give a balance, it's kind of like, and you probably heard about this. It's kind of like a requirements creep, right? Where you get a requirement. I did. I started doing websites back in the 90s. And I got a job with El Paso Honda right?

Speaker 1:17:19: Now we're like, oh, yeah, yeah, yeah.

Speaker 1:17:22: We're like, yeah yeah we're gonna make sure that the website is what you want. Okay, and it ended up working for about a month and it was a requirement screen. I mean, every time we met It was like something else. And this guy was like getting good ideas, but he was changing every single time. got to a point where I was like, we and the other guy, we hadn't slept for a while we're like, you know what, let's return their freakin thousand dollar check that we that they gave us and say, You know what, find somebody else. And we didn't even talk to them. We were so fed up and upset. We just signed return the check, went and gave it to the front office and see ya and we didn't we don't know how to handle it. But that's because we didn't have a good requirement because we want to be customer oriented. We want to be different than other web web making companies. We wanted to be the best right? And we're like, we're going to make sure that until you're satisfied he was never satisfied.

Unknown speaker 1:18:11: report format or example that you guys can provide. So like, feels like I think I understand like the goal the whole thing. But I think my quiet the most where i have more questions how am I gonna, like put everything all in one as far as the report.

Speaker 1:18:28: We have run out of time, but this is not gonna be the only time that we're gonna meet with you guys. We're trying to meet more often with the with the whole class and with the groups because, you know, you may walk out of here saying oh, I have a clear vision but then, you know, two days from now you're like, Oh, I really need to meet with those guys. We don't want that meeting to take a month. You know, we want to make, you know, make sure we meet frequently that we you know, we keep on redirecting to the same goal, you know from your side and our side that way the tools that you guys are up is actually you know is used by us.

Unknown Speaker 1:19:04: So lets thank our clients, thank you for coming. further instructions as to what you will be responsible for the interview report i know that Our clients gave a really good background and during the presentation they answered some of the questions in the q&a list that we have, we have another session that will happen at 1030. I will update you guys sometime today to let you know what is the instruction at when the due dates will be so that all that both sessions will have the information that each session is missing. So just wait for my email.

Speaker 1:19:45: I can take notes and everything right. So this is the main system right? This is where we're not going to give you a lot of like very specific things of how we wanted you to design it. We need help with this. But we will give you how we want the the the those reports right and exactly what we want. So you'll know isn't, but here

Speaker 1:20:05: we want you guys to be creative?

Unknown Speaker 1:20:06 : Yeah, be creative and then see what based on, okay? and if you have more questions put them in there. And then what we're going to do is we weren't very good with time hopefully for the 1030. Class. Yeah, we'll be a little bit better with the time. But uh, we're gonna we're gonna sit down with missionaries and when we meet with you individually will make sure to address those questions.

Speaker 1:20:26 : Hey, guys, I'm sorry, just just real quick. I just I just want to know if this was actually helpful the way we explained it or, or maybe there's something they'd like for the next two classes. Maybe we can make sure we go first.

Speaker 1:20:39 : Should we just start with the question? Yes.

Elsa 1:20:41: Will talk about later

Speaker 1:20:44: Sounds good to me before this. I thought it was gonna probably the man on the software. I have an idea.

Unknown speaker 1:20:50 : Just remember, stability, accountability and report generation

Appendix B

The following transcription was made from an audio recording made by one of our team members, Fernando Marquez, who was also our team representative during the client interview during our class session: 10:30am - 11:50am. It's structured in a way that readers are able to see who the speaker was among its corresponding timestamp.

Speaker 00:00 What happened?

Speaker 00:02 Their app failed.

Speaker 00:05 Their app failed. Why did it fail?

Speaker 00:08 They didn't test it well. We don't know.

Speaker 00:12 We don't know how they tested it right but I do remember that in the cyber security world, a few weeks ago they were like, hey who tested this? does anybody know what company tested this? Was there any cyber security testing? Was there any low testing or and nobody knew what was going on because he was kind of hush hush this shadow company, that was the name of this company, and so what ended up happening is that probably the guy in the the few individuals that that developed I'm thinking they tried tested it as much as they could with what they had in what they could think of right. But they never went really operational. I don't think that they may or they may have not I don't know, you know, go to I don't know go to high school and have 2000 students say okay everybody download the app right now. And then give you this quick and everybody just take the little quick survey or whatever and send it to the server. And then you know, just something that is operationally represented level it's going to happen, that probably didn't happen. So this is always very important. So when you develop code right, and if you're developing an app, and you run out of ways to test it, take it to your abuelita and say, Hey, abuelita, I created this app. Don't worry about it, how to use it. And let me tell you the first two, three things that she does you will be like "why did I not think of that?" Right. And that's operational represent.

Speaker 01:19 Yes, real quick. Before we move on to the next slide, let me do a small commercial. What are you guys doing tomorrow?

Speaker 01:26 Writing a report on this.

Speaker 01:28 Going to the career fair.

Speaker 01:30 Going to the career fair okay. Think about the job. Getting to meet the DOD, the army recruiters. Yeah, go ahead. And you know, you guys are on the perfect stage to start going and meeting the recruiters out there and you guys are situated in a really good position as I was recruiting at Socorro, New Mexico, New Mexico tech two days ago, I was recruiting at nmsu yesterday and I'll be recruiting at UTEP tomorrow. So get to know who comes here to university which type of jobs are out there for you. Right to center to start attacking to see what is which positions are available. A lot of recruiters, Let me tell you are looking for computer science majors, okay? And we are too so we'll be more than happy to take your resumes tomorrow, you know, back into your other different, you know, opportunities with our department now, you guys have been working on a project like this, you know will have some advantage over some other students. Please use that to your, you know, to your benefit in whenever you can be with us with anybody. Yeah, I know you talked to other other recruiters, you can put this on your resume. So you can like hey, I went through the whole requirements and develop software development process on a natural system that will be used for that is being used by the US Army army future's command, you'll get to know this and see the development plan.

Speaker 02:50 Okay, so this is just a little bit of what we do vulnerability assessments, provide mitigations and vulnerability support decision making and homework and we're going to be concentrating kind of on the on the pentesting. Okay and cooperative we put the quality because we work with the project managers, which are usually the system owners, right? So let's say you were going to go test Excel and, and Word, okay, we're going to go test the applications themselves, we're going to they're going to fly us over to Seattle. And we're going to meet with the product manager who's in charge in Microsoft of those two products. And that's, that's what this that's what this is. So we have a few minutes out, you're going to become more acclimated. And you're going to know more about this as we go on. But this is basically our process. Okay, when we're going to do an assessment, we have the…

Speaker 03:39 well, it is an like an event, let's say the calls from, I don't know, somewhere in the continental US and they're like, Oh, we want you guys to test this time. Okay, we go on an event. Right? And we've got, like, there is a pre engagement right interactions in the US if you wanna…

Speaker 04:00 I guess just real quick. When we say I guess terminology wise when we say system, system essentially to us is more of a system under test. So it could be essentially like a network of computers, it can be networked devices, it could be a vehicle that could be your radio, tactical radio from Iran it could be a GPS, and it could be software, it could be web application. It could be some other type of software that's out there. So so just Just be careful because we're going to throw that around. I know that was a question in the previous classes. What is the system so when we say system, we're referring to a system under test, again, it could be an information system from your laptop PC server within it could be an application, it can be a virtual machine within a server essentially can be like an enclave which is like more of a boundary like different like different types of networks within an area. So just just be cognizant of that. So…

Speaker 05:00 We got these reengagement interactions, right? And this you can apply it to almost anything that you do, right? So you can apply it into this class, right? So the system under test for for your instructor rate is you guys, right? She's going to be grading you guys, she's going to be assessing you guys, she's going to be giving you requirements, she's going to give you a task, she's gonna get stuff right back, she can go to the next class, that's her class and start bringing them right, because they're out of school. So that's basically that's basically the system. So we've got an intelligence gathering, you know, okay, what do we know about going back to, to Word and Excel? What do I know about it? Who's tested it? What's out there? What's vulnerable? What can I do with it? And so you do this intelligence gathering in the military, you look at you look at different countries, what countries are trying to attack the system that we're looking at, and so on, right? So the system can be anything, and then we get prime model. Okay, now that we saw Word and Excel to give us an example, I know that I saw this YouTube video of a guy who used to put a certain characters in cell A 102, and he was able to To touch this, that game of Excel, the now allows them to get, I don't know, whatever it is admin access to the process, we're going to hack the system, right? So so you're okay, that's a threat, that's probably a venue that you could use to to attack that system. Right. So that's the third one. Now, here, this this next part, this is where Frick is going to come in, right? where we actually do the vulnerability assessment. The movie analysis, assessment is usually a five to five day event, it can be a 10 day event, or a 15 day event, but it's usually five days, where we go in there we go a team of anywhere from four to 10, depending on how many system, how many individual components you have in that system, so that we can assess everything and then our requirements. And then from there, we usually have like, you know, daily, daily, daily hot washes or daily presentations. So let's say that some was she was our pm or our program manager. So she is our customer, right? So our lead let's say Oscar was our lead and Angel and I were were analysts. He's going to give us the task of what we do. At the beginning, right and then we're going to be reporting back to him. And then he is going to be reporting to elsa. So…

Speaker 07:05 Basically I am going to have to do a presentation every day of how the, you know, the vulnerability analysis is happening. And sometimes I may or may not have time to go and sync up with each of my analysts. That's why it's so important. Because having that repository of information I can easily say that go outside look, today, we need this is that this whatever is more important that I see from what they have done through the deck.

Speaker 07:28 And so right now what we're doing is we're doing a lot of time wasting, right? Are we going Hey, Kevin. So what did you work and what did you find out? Today? What are you working on you? Like all you I found this and I, and I, I know that this is vulnerable and whatnot, right? And then I'll go Eric, you know, what did you do and I'll be taking notes right? And then I'll go sit down and have everything up and put in presentation. Just imagine I just wasted like two hours right? And I took some time from you also, valuable time and then and then let's say that I didn't have to do that. They're not like Hey, guys, you know what? I need everybody to stop everybody. Let's go to the hot washes, go to a presentation. And I'll be like, Okay, so now Kevin is going to tell you what he did. We'll go ahead, Kevin, and we'll start talking right and over here. Okay, Sergio, Sergio is going to talk about what he did. So now we're there for an hour. Now it took four hours, right valuable time that he could have been there assessing the system over there briefing stuff. And not only that, I just cut your mojo, right? You were this close to break into the system, and you had all this knowledge. And now you went over there. Now you come back on it was like, you like oh, shoot, I don't even remember what I was doing. But what I've been doing for dinner, and when I we just lost, you know, so this is where we are, we want to help. And I think we're going to go to one more slide. And then we're going to go to the q&a session. So this is the thing again, once we start reading more individually, okay, more questions. And once you get this free, it'll, it'll make a little more more specific, a big, a big.

The big end goal to always is this, reporting this to the customer, right? Not only having the testing system of when we're doing the assessment, but having those reporting vulnerabilities that give us a good gives us a good product. So I don't have to be asking you each one of you what you did and having to type it up. And then, send me the this is what we do right now. I have 10 people. Alright so I created a folder, just draw your draw your artifacts, all your evidence, right is whether it be videos, whether it be laws, where the whether it be snapshots, and then I'm trying to put it put all those together with what he told me, I just wasted I spend like half a day trying to get into that or I could have made a system for you just you do you do that yourself right and I'm really good and everything and then you just update me and now I can update her. And because you know she's she's my customer and then when we go to the final report, okay, and this will answer maybe some questions right? At the end of the five engagement or whatever it is the last day we do what it's called an ER D, which is an emergent results brief. Okay, and that should be Something that comes straight out of written.

Speaker 10:02 When she wants us to update the update her. That doesn't mean you come and tell me, you know, but your system will update my system that way I can just go through your notes from my system because I already know which vulnerabilities you found, you know, if you have completed the tasks that I assign assigned to you, or you know, what percentage Are you done with those tasks? Or if you have any notes pertaining to those tasks?

Speaker 10:27 Yes, and, and then and that whole. So that's, that's the first thing then two weeks after that we do another one, which is called a risk assessment, and we send that to the customer. And that's usually just like a big spreadsheet. We may be a few comments of what we found is similar to the ERB, the ERB has they are because it can have different fields but it usually has the vulnerability the systems that affect us with a system like these, this is domains, what impact it has, what level of access that we get to the system or why is it important and then we usually grade it as a medium or high. I will give him like some type of priority of how Important it was, we go back two weeks later, and we sit down as a team and we grade each other vulnerabilities of whether it's high technical impact, is it and then is it high is it is the impact high on the whole mission? So let's say you have a car, the mission of that car to transport you from your house, to wherever you need to go, right? hospital school work, right? So that's the mission of that car. I hack into your car, and I'm able to get into your dashboard and show you that your tank is empty, and and the lights don't work or anything, right. So that's a very high technical impact, because you're not going to know what the hell's going on. But can I still go pump gas and just make sure that it's right, can I still can I still drive to where I need to go? Yes. So the overall impact to the mission may not be very high. It's a high technical impact, and it will degrade the system a little bit. But the mission I can still accomplish the mission in military terms, right. My mission is Whatever it's going to be right? Is it going to be to control or to kill the adversary. So I want to see what that's going to do to the mission, right? Again, we're going to go to each one and then grade them and then give that to the customer and say, even though I got rude on this system, and I'm owner of that, and I can do xy and z, you can still accomplish your mission. So that might not have the highest priority of fixing right away.

Speaker 12:23 Yeah, and like I was saying, we tried to meet two weeks after but our job is very high tempo. So today, we may be the three of us El Paso, but tomorrow, you know, actually next week, I'm not gonna be here, probably Angel is gonna be out of town too. So the lead gets, you know, gets to say, oh, man, you know, I need to grade out this. How can I get a background on what happened? What is you know how the dismal vulnerability affects the system. So thanks to those notes that we could have done at the event. He can go ahead and now say oh, this is high, this is low. This is medium, just based on the notes that he can read off now. From from the system

Speaker 13:01 so so at this point, go to the next slide. Okay, so, how do we start it? Do we how do we individually have general questions? Okay, question number one. Let's start with question number two. Okay. So who's gonna ask that question? Okay.

Interviewer 13:27 Okay, so is there a solution that you're currently using? And if so, can you provide a list regarding the current solution.

Speaker 13:47 Okay, so, we do have a current solution or a semi workable solution. Some of the things that we like, I think we've, we’ve, we've identified on the RDD. We didn't want to show it to you and we don't want to show it to you necessarily. Because we want you guys to come up with, with, with new things and new ideas. I think one of the things that I like a lot, I think that the likes, you can extrapolate from that documentary, which I personally you guys, I'll first tell you a couple things that I like. I like the fact that, that you have one thing that I can sync that everybody because everybody's going to sync, everybody's gonna have the same, which is a common operating picture. Every person has the same picture at any one given time. I like the way that I press a button. And it syncs my information to yours and yours to mine. Okay, so I give this list of vulnerabilities. I like the way that it allows me and allows you or me as a lead or whoever to take it for as much information as possible and give me all the artifacts.

Speaker 14:43 this is this is very important because I may get pulled as the leader of the event. I may get pulled by Elsa, and then now somebody else has to do the end of the day presentation and if they don't have my information, they're just going to be able to present on what they worked on.

What do you like?

I just what I like is the ability to be able to, for the analysts to write what it is that they've done for the day. And not only that, the artifacts of the screenshots, they've downloaded documents have credentials on there. So that that will be there as well. So I mean, that's for me as one of the big things is, is I mean, and that's, that's what's generally needed for for the report writing, or manual not only report writing, but for the, the ER b's, or whatever it is that we're doing in order to communicate our findings with the customers. Yeah, what I like is the fact that it's like a central repository that can hold pictures that hopefully. You didn't want to hold videos to like no, like, Oh, this is me. You know, exploiting this vulnerability in kind of like a new walk through that way, whenever the lead's briefing, the rest of the of the room can actually be more detailed,

Speaker 15:55 There's no limit to what you can upload for a given, you can have as many artifacts as you'd like.

Speaker 16:03 So one of the other things that I like is the fact that there's an accountability aspect to it. Now I know if someone did some type of a brand some type of exploit I know who said branded, if it was successful and I know what it is that he was able to get, maybe was unsuccessful. I know that as well. Why because why is that important? The whole accountability aspect. I mean, there's there's a lot of times when we're actually tasking and then the pm comes back and says, Hey, you guys broke something. And then you go back and you're like, well, what is it that we broke this all it was the service and then we go back that we actually touch that service? No. Okay, so so is a wasn't us, but then people go well, we did touch that server. So what do we do? I mean, the whole accountability aspect of it is a big difference.

Speaker 16:51 And samarah, based on what you heard right now. What do you think our likes are?

Speaker 17:01 Your likes.

Speaker 17:03 So what we were telling you right now, what do you think? What do you think we were talking about?

Student 17:10 the finding details?,

Speaker 17:11 The findings, did you notice that everything was here? Any think or guess why?

Speaker 17:19 Important information? Most important information to what you do.

Speaker 17:28 You could say it's the most important permission. Sure. So the The answer is that the current system that we have is heavily It was developed to first do this. This was an add on there is I don't know if you guys have used it yet have you guys with the task. This is something kind of new there was no that it was never finished. It's kind of like somewhere in the middle. But this is what most most of us are more familiar with. This part. There's a lot of people haven't used it and it's again, it's not working. It's not working the way we wanted to use. But, but this is this is this a feature that we need and that I'm sure once you start liking

Speaker 18:02 okay, let me let me add this real quick. I did like the flexibility that it has. Because like Angel was saying, once we reach this point that we're going to the event, right, and start performing the vulnerability analysis, you get a pretty good idea like Angel was saying, probably you have like 60% plan of the whole event, right. But as you start going through a vulnerability assessment, new things come up, right. So what is nice about the previous system is that you're able to add new tasks or add new findings or add, you know, different things. So that is that is good that the analysts can add new tasks and also the lead can add new tasks.

Ms. Elsa 18:41 next question. For users section on question number three.

Student 18:47 Okay. So the RDD stated that there are two types of users, the lead analyst and the analyst. So, could you please elaborate on the difference between the lead analyst and the analysts at about their privileges.

Speaker 18:58 Yeah, we'll, try to … let's because there's a lot of questions. Do you want to talk about this one?

Speaker 19:07 Okay, so the lead analyst essentially he's gonna be he's gonna be the one that's going to be getting updated with regards to what's happening, what hasn't been done, what findings have been been found. The analyst his main goal is going to be that you're going to be performing the task is going to be inputting what he did, what he found, what he didn't find.

Speaker 19:31 Yeah, and and then as far as contributors. So the way we work, usually the whole team right now, we all have root privileges to each other. So everybody has admin privileges, okay? So it's just kind of like an understood how you got a lead here, right? And you're like, Okay, I'm the lead for everybody's sync with me. But that doesn't mean that you can't sync within yourselves. And when I when we see once we say sync as you're going Give me all of your information and you're going to take all my information. And even though I'm the lead, I'm going to be seeing the exact same thing that you're seeing at some point. Okay?

Speaker 20:08 So this is a high trust environment in which everybody trust each other, you know, hundred percent. I mean, not only that, because I mean, for instance, let's say that Robert over here is working on something. And I must say, the next day he gets sick, he can't show up. So Julio, you're gonna have to pick up the pace, you have to pick up the slack. So you have to go in, you're gonna be able to you have to have access to what he did in order for you to continue on to work. So I mean, that type of stuff is what we do a lot.

Speaker 20:38 Yeah, end up in just flat on like, like, for example, yesterday, when I was doing an assessment, I was doing it for White Sands. And then something came up. Let's say hey, there's this system. That's, that was just like as that it's doing something. And then we looked and it was Eric, working on it. And now, where's Eric?. Oh, he went to the restroom. He hasn't come back and they needed something right away. So I go to his computer and It's locked. Right. But since we're working the stress environment with me as the leader or one of the analysts, and we know the passwords we're in a trustul environment, we get into into his into his system, look at what he's doing. And then we can we can, right away, stop the attack that we're launching or whatever, whatever it was.

Speaker 21:20 Yeah. Very trusting environment.

Student 21:20 The question I have a couple of parts. So how will the system differentiate between two I guess so since it's a trust environment, it doesn’t need to differentiate

Speaker 21:29 it doesn't need to differentiate however, we could, if you like I'm thinking of another system that we have for we have a kind of like a server/client where it has a little button that I press server and who's a first server. Nobody else can first server in this. So we know that I'm the server and others when I or at least when I when I sync to everybody, you know that this IP is the server and unless I release it, then somebody else can be a server but Again, we have this like this, this is the way we want it to work. But if I get out of the system, if I need to take my system out of out of this, because I'm whatever I need to do, then I'm going to say, Hey, I'm gonna say, hey, Julio, I want you to make sure that in 30 minutes you sync with everybody because I and then when I come, I just want to sync to you. Okay, so then he leaves. Now he moves, we'll see system here. And now he's everybody's going to be syncing to him. Okay. But again, it's just something I kind of like understood. It's not technical, we want to very, very flexible. So you could potentially put arrows here from everybody, whoever that is

Speaker 22:34 just just real quick. This is where that's actually very important because we need that redundancy. So we need to have everyone essentially needs to have the data. Why? Because as one of the things that we do, we're constantly tasking we're constantly re imaging threats. So that means that the that the rate of our drives failing is, is high. So like if your drive fails, and we will essentially lose all the data, but if we're syncing With everyone, then essentially we can I can give you like a new drive, and then people will sync to you, and then you'll have all your information back to you. So that i think that's that's a really good point. I mean, everyone needs to have data. Why? Because we need that redundancy we need, we need to make sure that people have the information to have the data, or else your hard drive fails and what I mean

Speaker 23:22 So, no other privileges and no other users. It's just it's just a leap, and it was really surely user. But again, looking at it from an OS perspective, we're all admins. next question.

Speaker 23:41 So, what would be the typical scenario of use by lead analyst and by an analyst?

Speaker 23:48 Okay, so, I mean, they're very, they're very similar. I typically used to be again at the team lead computer security lead. I give you all the tasks right and and I assign the task, right? I know, okay, I'm going to do these 20 things. And I got to call these systems and I go through these 20 things on all those systems. So I'm going to say, okay, Eric, we're going to do a one to five and I want to assign you a task. And then Alex, someone assigned me the task, right? And then I'm going to go with with the other, Eric, we'll sync. And then we'll say, okay, you're going to release tasks, right? And then I'm going to sync to you: “Hey, i’m gonna update my task”. And then I have, I have a scenario here, where, where I have a list of all my analysts, and I'm just gonna say, and it's gonna, my system is going to SSH or s&p or something right. And it's going to update your system with all the tasks right? And then your your use case right there would be okay, I got all my tasks. And I'm going to take this first task, right and in that part, we need help with as far as the progress of the task, it could be a okay I'm working on this task you have like a status as I don't know progress or or percentages on however that that we'll talk about as we go. So you'll, you'll have that task, you start working on it. And then at some point you're going to say done, or I'm completed and, and then that task may or may not produce a vulnerability, Okay?

Speaker 25:15 And that task may produce I produce more tasks sub tasks, right? Maybe you're looking for vulnerability on a printer. And by doing that you found the vulnerability of the network, then you add a subtask saying, hey, look at this on the network, I see maybe a potential vulnerability that I want to look later on. So you get fooled somebody else that has that information comes in like Oh, you're working on the printer, but he said also to take a look at the network as they're there may be something

Speaker 25:43 so you have to do this and me as a leader. I can tell you Okay,I want everybody to sync at the end of the day, he may say, you know what, I need everybody to sync every hour. Or not. Can we say I want you to sync if you find something, sync right away, always think sync away. If you don't find anything, don't worry until the end of the day. So those are the different types. Next question.

Speaker 26:04 Okay. So are there further privileges for these users not mentioned in the RDD?

Speaker 26:10 No

Speaker 26:13 are there any other types of users not mentioned in the RDD?

Speaker 26:15 I can’t think of any more users

Speaker 26:18 It's the next question we have is, how many lead analysts are allowed per cyber engagement?

Speaker 26:20 Okay, so for that, it depends on the scope. So So essentially, you have a big scope, then then, then you can have anywhere from 10 to 15 analysts. There used to be an engagement that we should do here at Fort Bliss. And we're so so that was almost like a very big engagement. And we had like about 15 analysts at a time assessing why because it's a big network. We can, we can do a task like for instance, I'll be doing a task in two weeks and only two analysts. So it depends on what, it depends on your scope.

Speaker 27:01 And now I'm going to contradict what I just told you. Any other user, right? Yes. So that would be a scenario where you have a team lead. And then you have technical leads. Okay? Now, the only difference is that that the the team lead is going to oversee the whole thing, she's going to be interacting with the customer, and whatnot. And then the technical leads are going to be interacting with the team lead, because a technical lead will have another little group. So just imagine that this is the technical lead, right? So technical lead will be in charge of those four people. And then we'll have another type of lead in charge of another four people, right? And then you have the team lead, who doesn't want to deal with all 50 people but just wants to deal with the technical needs. It really doesn't change anything else is more of a of a name of a, you know, whatever. And the way we would work it is not necessarily technical, but it would be like okay, guys, I'm only going to be syncing to you for a page so I'm going to add you for to my sync and when I sync I just want to sync to you and I'm gonna I'm gonna rely on you guys to be syncing with the others . Now, a lot of times, a lot of times we're not co located. So the syncing may have to be I may have to carry my computer because I'm working in a secure environment. And I got to go to some other secure environment. So, so assume that we're in the same physical network. Okay.

Speaker 28:21 So a follow up question.

Robert - student 41:42 Umm out of El Paso, Texas. Please provide a definition example for the following concepts describe the current processes used to create them and the relationships between them, especially when you guys want to relate two tasks together, what type of things are going down so the system how does it relate?

Speaker 42:01 okay so the system we kind of need to kind of talk about right? umm Where we usually having set defining the system under test, right? We have another tool that or we could put usually it's by IP address which you say okay this IP address this is the whitelisted meaning we can test these. These are blacklisted meaning we cannot touch those we'll see them and we can test them if we wanted to but those are of out scope so that's usually the system right your balance what can and can't I. What am I what was I hired to do basically and what systems should I be touching? Okay, okay. So that's the system. An event. An event describes a natural assessment that *5a * prevent I'm telling you. We call them an event or we call them assessments, or we call them penetration test. There's different flavors depending on what organization required. So Congress came down with a, D.O.T. and E policy, which is director of. Director of *testing* operational dissimulation. Yes and there's, there's other requirements on depending on those, they have their own set of requirements. But the assessment of the event, they are basically the same, so the event is the actual when we are actually

Speaker 43:11 they are like the dates, right that *you get* over there with the system.

Speaker 43:14 And and and the event, also, you're going to be seeing that interchangeably, but you have a project that may take three to six months, you know, to accomplish, but the actual event is that one week, where we're going to be there touching the system hands on and we're going to be hacking away, or, or or doing vulnerability assessment of that system, so that's an event. Ummm a task. Okay umm. So we have any event, and we have a set number that, you know, technology changes over time. Let's say we have, in fact, I was looking at an event that I'm doing, I think we have 13 different tools, or 13 different apps or programs that we use to assess that system automatically. So we run on each manually, right? say, okay, we're going to scan the system. And that's going to check all your ports. And then seeing what what what ports are opening, what ports are closed, what technology your using, we have others that are going to try to see if you're using any default credentials. And then so on. So you have those, those tasks, those umm. Those tools that you have to run. Now those tools have to be run on all or maybe some set of systems. That's where that tasks come in. Right. Me as the lead. I know what I need to do. I know what I since that's with the PM, the product manager, she told me what I needed and I know the requirement that I need to do and identify a set of things that we need to do now I need to organize it right? That's what the *team* um. Okay, I have four analysts oh somebody got sick now l three, right? So I put up the tasks come out of there right. So the task could be like, okay, run these 13 tools on this system, that can be a task and then second would be like, okay, based on the results of those tools, like look at the critical and the highs if they're identified as the critical or the high. Or look at the results, right of those systems and see if we can find a vulnerability. So those are the subtask mean of those tasks so you could say, okay, run to one, which is a vulnerability scan. Subtask look at all the critical look all the critical findings from this and, and umm see if they're true positives, right? So that could be a subtask analysis. So going back to the word and, and it sounds right, you could say, okay. Subtask, task one. Open and close word. Subtask, right, create a new file, and export it or save it as a PDF, save it as a CSV or whatever, save it as a doc or a docx, whatever. And so those are could be subtasks of that first. And that's, that's very flexible and that's nothing necessarily that you need to define, but just have the infrastructure there so that we can implement the door. Umm. And then a finding, okay, so. Go back to the other one. To this one, so you have all these tasks, right? It could be that I go through 100 tests, and I have no findings, okay? Because a finding is, hey, the system was not able to save into PDF file or Hey, when I save it, when I save it to PDF right? Guess what it took me to this website where I can download free movies, okay, or things that the system was not intended to do and that you know it's vulnerability, right? So that, that would be a finding. Okay. Another example of finding

Speaker 46:48
just just real quick, kind of like a step back when we say we find, findings for us and are are are essentially vulnerabilities. One of the things that we want to look at when you claim It's a vulnerability, we have to actually be kind of your typical definition of vulnerabilities and weaknesses in the system, we've had to take that a step forward, we kind of use to use the old terminology. And essentially that for us is this is a, susceptibility. So vulnerabilities, not only is it a weaknesses within the system, but something that can be exploited. That's very key for us. And when we're doing our testing, if we can exploit something, then we say it's vulnerable.

Speaker 47:27
And basically, you're bad. It's the validation that the system is vulnerable, and it can be attacking this this manner. So that's why it's so important because you validate right right group that you show over there. So essentially, that's what Juan's kind of getting at is that you can you can have all these tasks, essentially, you have no finding because, I mean, there's no nothing that was vulnerable that you found. But I don't know I mean, that's something that I want to do is kind of differentiate between, because somebody could be vulnerable and there may be something less as fine that something says hey, maybe this is something that you should watch out for. It's not necessarily vulnerable, but it's might be an issue down the road.

Speaker 48:07
Yeah. And that would be that what he's talking about is like, let's say you have a vulnerability that you were not able to exploit by your like if you if I know that because everything like you want to break into a house, right? Not that people want to do that. But let's say you want to break into your own house because you're locked yourself out, right? You know the vulnerability at your house, you know, that you always, always leave or your wife or your husband or your mom or dad or whatever always leaves the kitchen window a little bit open because of the odors and most of the time it ends up open. So you know that more than likely that's going to be open. So you go and check that, right. So you know, that's a vulnerability.

Now, when you're in, you have exploited the vulnerability,

Now you get in and now you're like, Oh, that's for sure a vulnerability. But now you go and you're like, oh, shoot, it's open, but I got to stopper there and I can't get in. Right, then you know that. It's a potential way in and it's already there. If I don't take the screen out and I put my hand or get some object, I might be able to take the stopper out. Okay, but I don't have. So you might want to put that as a finding. But that's procedural. That's nothing that affects the technical. Okay? That would be more of a Hey, guys, if there's something or for you, as an analyst, you're going to feel strong about, hey, this amount of finding, I was not able to exploit it. I was very close to this. And then we have those discussions. And then we'll say if it's if it's, it's vulnerable or not, but it's very important to differentiate that. Politicians not to get into politics. Politicians see in us people a very, very exploitable vulnerability, okay. And that exploitable ability that politicians always seen in us is fear. If we as a politician can get fear into your body. Right, I've got you. Okay, because I'm going to exploit that fear. Right. ahh all those Mexicans are coming from the other side, they're going to come and they're going to kill us. All. Right, that's a vulnerability. Right? And then and without political parties, right? And then the democrats would say, Oh, you know, all those border patrols, they're just killing the poor kids that are coming from other countries. And putting fear, right? That's, that's, that's something that politicians do. And if you can get fear into somebody, you start controlling those people. So make sure that whenever you feel fear, step aside and say, Okay, wait a minute, let me not go by feeling let me think about this. So that's, that's a good way of saying what something that's, that's vulnerable, and you can exploit. Okay, you can go the other way and say, Oh, look at all the people that come from Mexico. They're so wonderful. They're teaching our kids and everything.

It could be a vulnerability, but I can't really exploit it because people don't care if we people come over from wherever, right? We care. And that's why the news are very negative, right? Because they want to put fear on me gets your attention, right. So that's kind of like in a system. You see a system you see a vulner... vulnerability, right? And then if you if you if you're able to, to exploit the vulnerability, but it has no impact on the whole mission. Okay, let's say I want to send. Did I give you the example of a car, right? No, no. Did I give it here or the last class? It was here. It was here when we were driving. I don’t even know. Okay anyways, so that's that's a good thing. Right? The mission right, make sure the mission over.

Speaker 51:25
So just just just a real quick. I mean I don't want to confuse anyone to be honest with you I'm not sure of the entire requirements that we provided to you guys. I'm here more of a user, a lead as someone that has more experience that that needs like of the wants and the needs for for for for for the for for the project itself. And I just kind of want to sit back and say yeah, findings are good, but we do want to report issue. And the reason I say for that is that for instance so I kind of gave the example and oh at fort bliss we use to do a big test that we use to have 15 different animals, we should do it like twice a year, see the first iteration of the test, we found an issue like, hey, there's some data that's going back with we can we can't, we can't exploit it then all of a sudden, but by the, by the time the next test rolls around, which is in about six months. And you know what there was this tool or this exploit called Harpie that came out. And you know what this is, we found this issue, but we couldn't exploit it because there was actually no, no, no exploit code available. And now you have the exploit code and then I need to kind of go back to your old results. Oh yeah, it was it, we did report it, we kind of recorded it but we couldn't exploit it, but now we can. So now it's so when we recorded it the next time is that when it goes from being an issue to being an actual vulnerability why? We're now able to exploit the Harpie issue.

Speaker 52:50
And that's why it is, so important, right to keep that repository of what happened on the previous event because we want to carry that information with us. kind of do the lead before we're going to say then you go review what was done last time. And you can say I want now a new task for this iteration of the event, I want you guys to focus on these vulnerabilities because now we may be able to exploit it

Speaker 53:13
So you had all these tasks, you are going to have some findings, right for the next time around, because usually you test that you you umm take a cycle, right, you test and you test the same system over and over through the years. So now the next time I go around a lot of my tasks, right, yeah, they're going to come from the test plan, but a lot of tasks are going to come from these findings, because now I know for sure what was vulnerable back then and I want to go back sometimes we do a what I call a verification of fixes, V.O.S. or Vos, and and all the requirements are strictly mapped to a to a finding for finding comes and now we have a task. So that we when we go re-test, we're going to go specifically do the tasks that relate to those findings. So it's one of those

Speaker 53:55
This is very important because as we only have that week, you know if you're going to do it again, you don't want to do everything all over again, you want to, you know, pick up where you left. And you know that way you use your time more efficiently and actually move forward on the testing?

So this so this finding umm this finding findings, I guess it's more on the findings section, right? I guess, I would say

Elsa 54:19
True, I have a follow up question. So do we need to actually introduce another concept or umm and make a property called different types of finding? So that when you guys generally record as the lead you will be able to say, hey, those are the actual vulnerabilities that have been exploited, or some potential issues in place on definition, you guys saying there's like two ways of findings

Speaker 54:39
I would say no, let me tell you why. Just because I would say as long as we have each finding. That we can give it I don't even if we even need to give it a priority, but we don't do that. What he was talking about more informational, right? We have these 10 vulnerabilities that are we verified our our our exploitable and then we have this one that might but we just want to carry it over. That's that's a special case but it wouldn't be good still we would still treat us a vulnerability because on the report we want it to come out and it's just going to see for informational purposes so

Speaker 55:17
And I think based on the screenshots now notes and if possible videos you know, attached to that finding, we can easily say like oh yeah, this was exploited or this wasn't exploited.

Speaker 55:28
So I guess what you're saying is whether to say something that’s vulnerable or something just an issue. Yeah so that I would I would

Speaker 55:36
Maybe like a button maybe to say, vulnerable or informational

Speaker 55:42
Yeah because you're going back when we write a report we're going to get everything that's on free. So if you’re a vulnerability or vulnerability if you're not a vulnerability essentially we do provide that to the customer and we do tell them hey look, this is an informational finding essentially that’s what we call

Speaker 55:54
Maybe maybe a tag on it like to be okay this this finding is a Comfort vulnerability, or it's informational only, or other something, you know, something like that. That would be Yeah, you're right. But nothing that would change. It would be the same type of thing would, it would be a finding still in the findings. Any question question. Next question

Robert - student 56:18: Oh next question. It's on events. How long does an event last? Oh, yeah.

Speaker 56:22: Yes. What What do you know the answer to that? Whats the answer to how long of a event?

Robert - student 56:27: a week, the week week or weekend initially,

Speaker 56:30: and what are start and end points?

Robert - student 56:33: dissemination

Speaker 56:34: start date and end date, in the morning, usually Monday morning, and then Friday afternoon, and we finished with that ERB with that emerging results.

Robert - student 56:43: What are the different status types of a task?

Speaker 56:47: Okay, that I'm going to leave, we're going to leave up to you guys. Okay. We would like for you guys to do some research and the only thing I could think of and I have no experience in this would be like a ticketing system. You have a task and somehow goes to the end. And you could have statuses or a status or a i dont know pending work and I don't know. So we, right now the way it's defined is arbitrary from one to 100. So you would just it's, you would pick okay think about 50% done, but it's I would like to see what what things you could you could recommend or what options you would get

Robert - student 57:26: can I can a task be created without the assignment to an analyst.

Speaker 57:29: Yes, yes. So so a lot of times this this is how this is what happens you can either get there already with great already popular more than likely Monday morning, though, the because it's a lot of classified stuff. Monday morning, Fernando, who's going to be our lead is going to get there and said, Alright, guys, start doing nessus. Let me let me get all the tasks ready. And as soon as as soon as you are while you're doing that first task that is not FRIC. He's actually creating all the Tasks. Okay, and then he could be a control freak. And then Jorge could be more of a people person or more of a people pleaser. And Jorge and Fernando is going to say, Alright, this 10 Task roberto, you're gonna do it robert you're gonna do it. And then these next tasks Samira, you're gonna do it, and this guy Jorge is gonna say, Alright guys, I got the 30 tasks. So we're gonna work it, just look at them and pick whichever you want and start working on them. So boom when you go in there, and I want to pick this task and you start working on it, right?

Robert - student 58:32 Based on expertise that will happen to is like, well, I want to pick tasks three, four and five because I'm really good at doing those

Speaker 58:38: Okay. Okay, those are assigned. And then, and then everybody picks their own task, you let them and then you have these 10 that are not assigned and then maybe those you can assign. So,

Robert - student 58:48: yeah, so we want people to be able to pick this tasks or we also want the lead to be able to assign us.And then is there a limit to the backlog of tasks before New craft tasks can be created?

Speaker 58:58:

No.

Robert - student 58:59 Okay. What is the maximum number of sub tests that task can have?

Speaker 59:03: None I mean no, unlimited.

Robert - student 59:05: Okay, what is the number? What is the maximum number of images that can be attached to intensity?

Speaker 59:09: Unlimited

Robert - student 59:09: And what format? Do you want the date displayed in? One place?

Speaker 59:13: For that usually for for military? It's day day, month month year, year year, year so those six digits. But you see how we take, we take no, no, no. No slashes or anything, just because most of our work is done using Linux? Or Cali. Right. And the forward slashes would cause a problem, right? Because it's thinking that it's what?

Robert - student 59:41: Delimiter

Speaker 59:41: A delimiter, thats its what directory, right? It's thinking that every one of those is a directory. So it'll it'll it'll go in there.

Robert - student 59:53: I don't think I'm 18

Elsa 59:57: our software for task question number 18

Speaker 1:00:01 Yes sir

Student 1:00:03 Please describe a scenario where a subtask is associated with more than one task?

Speaker 1:00:09: When a subtask to be associated more than one task, that's a good question. What is that? That's one of the requirements.

Elsa 1:00:18 : So the teams

Speaker 1:00:19: I just came up with that question. So I am, I mean, I can think of, there could be three tasks that are almost identical, or maybe identical, technically, but they're just being implemented to a different part of the network. So you're going to have one task, thats going to be data collection, vulnerability assessment, whatever, right? And you're going to, you're going to do that on these 10 hosts for this 10. And then you're going to do the exact same thing that he's doing.

Speaker 1:00:53 And these 10 hosts

Speaker 1:00:56: and then you're going to do the same. Julio you're going to the same thing they're doing but You're going to do it. And usually the first space, which is all the information gathering, everybody's kind of doing the same tasks on a different section just to get all the information. Okay, and then usually on day 2 now that i have all the information. I want to come up with more tasks, or I'm going to have how, how have you helped me identify tasks?

Speaker 1:01:19: And usually like by day two you, after looking at those first systems, right, that were analyzed to the team leader will come up with all look, this is the priority of the systems based on the on the mission impact that they may have. So I want you guys now, because we have a Linux server, I want you to focus on that, because we have a Windows Server. Now I want to another tasking with you focus on that.

Speaker 1:01:42: So that could be kind of a scenario for a subtask too, but I can't think of one I guess. But do you see that? I want to give you that example, because you're task and subtask are going to be identical, or these three tasks. Does that make sense? They're not different tasks, they're just different analyst and doing it on different systems. Okay? Now, it could be that you find that when you're first finding is going to be exactly as his finding, which is going to be exactly as you're finding, because it just so happens that that low level system was found on the three submits or on the three subsections. Now those are going to be three findings, right that are going to be reported it might be the exact same findings, but they're gonna affect different components. So at that point, I could probaly Group them and say, Okay, this is one finding out the whole system, right in three different components. Does that make sense so so I don't know if I, if you could get information to answer your question. Next question.

Student speaker 1:02:46: Could a subtask bcome a task and task become a subtask and how would that work?

Speaker 1:02:53: Could a sub task. I would say that Yeah, subtask could become. If a subtask is big enough. They were like, you know what im just going to put it into a task. You know what, thank you. I'm going to have somebody else do that manually collaboratively, but that's a whole new thing. Right? So that could happen. So you elevate I guess that subtask. What tasks it would seem to me just kind of, you know, one, hierarche one level? And what was the second part of that problem?

Speaker 1:03:22 Yeah, if task can become a sub task.

Speaker 1:03:26: Yeah, I guess you could, you could, we could potentially do that. Just say, you know, what this task is actually related to now, this one, let me make you a subtask of this one.That would be, but it could it could be. It's not necessarily something high up or minus nessercially of something that could do but, but yes, it could be it could have the, the, I mean, if you're able to do that team to make it that flexible, that'll be awesome.

Elsa 1:04:00: So let's say I have the task, a sub-task And my analysts have already discovered finding a finding not attached to the sub tasks. What if the task sub tasks get promoted to a task will the findings be now attach the task or is even allowed in the system?

Speaker 1:04:17: I will say if it would follow that subtask that finding, right, because

Elsa 1:04:21: So It's possible for an analyst to attach my name to a task. If it has a sub task. I have a structure I have a task. I have one sub tasks and my analysts to discover a finding, so that finding obviously should be attached to the subtask and things get promoted how would you handle the relationship when you need them

Speaker 1:04:44: So I'm not sure I'm not sure what the relationship here is in there some technical relationship, we think, in other words, do we have a finding that says, Oh, this finding was found under this task?

Speaker 1:04:56: We usually have them separately, right, right, we have all the tasks and then all The findings Get over here. And because of the nodes, we kind of relate it back Oh, well, I was doing internal sense of the system I found, you know, this, but they're not directly linked or to two list two separate lists the way it is right now. And, you know, we were easily can go back and say, you know, these finding was related to this task, but it doesn't like it is not critical that you have that

Speaker 1:05:25: I guess thats the things And I never thought about that. But when you're talking about, about maybe a view or a space for an analyst, only that analysts could see on. But it wasn't that question, but I could see how you're working on this task and your maybe getting these artifacts and getting this information, but you're not sure if it's going to make it into a finding its going to be a real finding. And then, at some point, when it becomes a finding, then then you just I don't know, you just I don't know, put it visible put it in finding. I don't know. But for now we're not we don't we don't map findings to a tasks

Elsa 1:06:08: So for the system that the class is working on you dont link findings to a task?

Speaker 1:06:09 No, no, no your tasks is just what you have to do, and then whatever it comes out of there, you're going to be creating the findings

Speaker 1:06:20: I think that's more of a nice to have. And and I think, actually, I think it'd be a good idea if we can map it to a task. So whether it being the task itself or the sub tasks, or the sub tasks got promoted to a task, I think

Speaker 1:06:38: the way I see it is, basically you're doing your task, right? And then suddenly, you have a finding than you'll create, basically these finding, and probably you have a drop down list of the tasks and you can just select oh you know i did this finding by doing task number 11

Speaker 1:06:55 or task or task 311. Yeah, I can see,

Speaker 1:07:01:I think it's good because it kind of goes back to the accountability aspect of what we want for the for the tool itself. So I think it's a good idea having having a map to the task or subtasks

Speaker 1:07:14: What time does the class end?

Elsa 1:07:15: In 4 more minutes, go ahead and go to question number 21

Unknown speaker 1:07:29 : So, if there's an overdue tasks how's the lead analyst going to be notified and how frequently should the lead be notified

Speaker 1:07:37 : So that you could you could potentially put a scheduler for the need to say okay, just you know, sync every so often in wanted to right now right now it's more like verbal analysts and like, like I said before, some of them some some leads say, Don't appeal until the end of the day. Or do not update unless you or obvious as soon as you find something completed the write up. So, I wouldn't we shouldn't put a lot of like have on actual actual due date. I mean, make guess you can

Speaker 1:08:10: But I think that's a nice thing to have to be an alert to the lead, you know, saying hey this task is overdue by this much like

Speaker 1:08:20: I can see one scenario Oh yeah, I can see one scenario I have I have these 10 tasks. And I've got this one task that if exploited is like, huge right? And you're like, just give me more time, right? And I guess I can say all right I'm going to give you till Wednesday, but after Wednesday, you got to complete all those nine all the other nine. And so, you could say alright? And then that can be a way of managing your time and say, okay, by Wednesday, if you don't if you're not able to exploit it, then just leave the task, right? or leave it or say I was not able to exploit it and then continue all the nine of the other

Speaker 1:08:57: Now you know what, it's a good idea because from my from a testing perspective, that's, that's one place we're around as they get stuck in. I mean, they get tunnel vision, they get focused on one certain thing. We have 10 tasks to do. And then at the end of the week, they're they're still stuck on that one task. So, I mean, it's I mean, if that's something that can be pushed as a notification or whatnot and/or that, for the lead to know is the progress in the feature.

Appendix C

The following transcription was made from an audio recording provided by our class instructor, Ms. Elsa Tai Ramirez. This interview took place from 2:00pm - 4:00pm.. For quality purposes, this interview was broken down into 6 recordings by Mrs. Elsa, thus, timestamps differentiated from the other appendices.

Recording 1

Speaker Elsa 00:00 Finding is already attached to a sub task or a task in the current system already no?

Speaker Oh, maybe I'm missing the undersea put on, you know what it could have? Yeah, I think you're right I think drop down there or it was automatically
labeled. I don't remember it being labeled practical now they remember from the task you would say finding, and then it would bring up a finding a needle out and we're already like put some number from ID that was that was linking into it.

Speaker Elsa Because I know I remember there was a field that is called sub task and there's a drop down I thought instead of finding level or that's all we had another discussion about if the lead analyst is doing his or her work and then found something that he/she wants to capture then you could have orphaned findings. That's how that's how we came up with the idea of orphan findings. So, I would assume that because of the orphan findings, or the findings would have attached to something and the current system And…what was taken the orphan finding. You could have orphan findings. And then for both, so either have a finding attached to retire so or not, I think the scenario presented to me was, let's just say, the three of us are working, and then I already was assigned a task. And I found a vulnerability exploited a document as a finding to the tasks I was being assigned. To me, it makes sense because of showcasing that I actually completed it, assuming that I found something and I was able to exploit. And then while I'm doing so, let's just say I saw this other vulnerability that wasn't part of the task that I was assigned, but it so happened that I found while I'm working on it, then I could document that finding that finding again, it's not because of a task that I was assigned to say I was doing something else. And I found this other more ability to exploit it. So then that became an orphan finding.

So, yeah, I don't want to say, should we just captured as advisor? You guys are I think Alliance. I like it. I like having, you know, the ability to be able to touch it or not. Yeah

Speaker Elsa So that if we don't attach it then as an orphan finding and the later on, you could always attach it.

Speaker Right. Right. Yeah. Because the way that we have worked in the past is that when we do a finding on the event that I have been, the lead was not asked us to attach it. And then he will listen up everything that I guess he's the one that is very is very new, the taskings some people don't do it, I could see I could see a few events asking wouldn't even matter can I need to find me,

Speaker Elsa but then when you do the report, so, is there a particular structure in the report where you have lists all that. So, this is the tasks here as a result of this task. So, you just look at the findings, yes, also the task will matter at that time…

Speaker it only matters, whenever the lead has to explain how the finding came inside of the task and some don't feel the need that background information when he has to explain Yes, exactly. So, it helps, it helps tell the whole story, finding sources of finding to find this and then now you can put now you when you write the story would say, you know, while doing a scan on this noise, because one of the important things in the report is that we want to tell the customer, here's, here's what we found, here's how we did it. So you can reproduce it. So, so that's, that's how I would. That's what I would make. As far as my opinion, the tasking that's all internal.

Speaker Elsa Because this is the way I'm seeing it. The data that we're collecting, if we're able to structure it properly, it would make it easier, regardless of what you put on the report, internal or external, because if the customers they only care about the findings, majority of the time, you could just have view because we have the information the relationship established, you could just say, hey, just show me all the findings and then said and then if let's just say to lead this particular customers asking how do you actually derive it then you could have a another customized view for the report. Including the relationship between the finding and the tasks and the sub tasks.

Speaker And that is the case most of the times you focus on finding a new producer for that will be really nice.

Speaker Elsa Yeah, because I would So from my perspective, being present that information and makes more sense to establish the relationship as the analyst and the lead, are doing their assessments versus having delete, oh, I collect all the findings. Let me take a look at this finding associated with this.Okay, so the question was, let's see. There was a question that I skipped. I wasn't sure it was really answered. Question number four. Could you have more than one analyst per cyber assess engagement. Question number four. So then in class you guys talked about the the technical lead and the lead based on what's being described, there's really no difference. Exactly. So then by definition, you could have multiple leads…

Speaker Yeah,because they're all basically everybody has the same permissions in the same tree.

Speaker Elsa So then, what exactly could the lead do, that the analysts couldn't because there was another part that was a little confusing, as far as the thinking goes. So let's just say the four of us are analyst, and let's just say, Juan is the lead. So while we're all connected the same switch, do the three of us automatically sync our content to your computer and then you push your sub What are you actually pushing back?

Speaker So So When once once you send me your stuff, right? I give you a snapshot of what I have, okay? And then let's say, five minutes later he pushes someone get his stuff and he's gonna get a snapshot of what I have. Because that's my new stuff. And then he goes later now he's getting his and what he's gonna get back now everything that you guys push…

Speaker Elsa but then at the same time because I sync with you first so I'm not gonna get your content But you see, so that I have to resync this or?

Speaker well actually the way it works is you just send me your stuff send me your stuff you're sending, like do I have everybody's this?
stuff? Okay, hold on, and then you get it. Okay guys, I'm pushing back. Push back goes.

Speaker Elsa So then, if everybody's on the same switch, why do we need to do the constant pushing pulling against each other.

Speaker Okay, start finding new findings, completing you when you have done anything so then if just analyst to analyst, what are we actually sinking like everything that you have or you have an option to select Oh, I want to only want you to see this finding for free. Okay, so everything is so basically everything that you're having your hard drive you're sinking into…

Speaker as far as it goes with findings and tasks, right? everything within the free system.

Speaker Elsa Okay, so then let's say, you and I sync with the lead at different times. Same task, allegedly, we're collaborators. But at the time you sync with the lead, the lead had updated a description for example. So when you and I sync it's the same task. How is the system gonna know which one to… it should be actually the latest one, right?

Speaker Yeah, we have a similar problem right now with invade that, that are let's say, we're going to scan right. And then the scan is tagged with a with a date and an hour. And then we find out at the end of the day that there are some changes that were made on the system. So will you scan in the morning and then ingest that information again? We already scanning so the question was okay, does it have replays and what happens it just gets upended. This is fine goes down again. So we have like five duplicate. So that's a good question for the collaborator because I could see how difficult that could be.
I'm thinking the collaborators will probably lead to
I don't know sync amongst yourselves.

Speaker And then, I mean, it kind of goes back to what you had said was some type of Master, right? For master record that you want to constantly keep updating. And once right with regards to our other tool, we run into the issue possibly where people start population in certain things, but it's not necessarily no one else can see what they're populating. And then they don't until we have to wait until the end of the day when everything gets integrated. They see that then you'll you'll see like the what, whatever anyone else had like I mean, server reclining type model.

Speaker Elsa I guess I'm really trying to understand this whole idea of having a lead because it's really just a computer so if I put a computer here and I say this computers is the lead of all the analysts, we just go there whenever we update, we sync it we think it and the I guess we always sync through the lead, if we share findings because one scenario that Vince mentioned, let's just say I'm working on this particular vulnerability in this system, you have done something similar in a different system, I'm very interested in how you actually did it. So you share your your sync with me and share the finding and like to take a look at the finding and then do the similar…

Speaker or what has happened in so many events and like, I found these, these finding, I usually get up to somebody. So somebody else has more expertise. So what we'll do is I'll tell them, you know what, let's collaborate let's sync together, he gets the funding keeps on working on that right go and work on something else. Then later on, when he completes that finding, he syncs to master then I sync to master I got the rest of the story was done right. So in that case, as the finding especially you pass what you have done to your part, but I kept one copy of it right now the copy and then he keeps on working on it. He's updated, more stuff to play.

Speaker Elsa But what have you let just I don't know how much communication? I'm sure you guys have a lot of communication in person. So what if your partner is synced with the lead? And then you didn't know that he had synced? So you went ahead and sync the lead? Then are we checking just timestamps? Yes.Okay.

Speaker And then sometimes I have seen it that you have the two you have my outdated and you have the new one. And then we just got to go in and erase the outdated one. But that's a manual process so that we don't erase it

Speaker Elsa I have asked Vince another scenario where the outdated version know the updated version got synced. Because timestamp is a while Okay, so timestep What do you mean by timestamp? The last time you saved it?

Speaker It's a timestamp of,of the product right? So yes, when they are That was that it was that you said. So the way we took on that problem that we were having with our system is that they have Port 22 open, and I go into something, I was able to login or default credentials submitted, it has a timestamp, and that doesn't get updated. If I then find something else, we're going to have to click a timestamp. And this moves down and timestamp might enter more information. So the timestamp companies a snapshot of what you enter at a particular time.

Speaker Elsa Also, it's not just the time and the date, but there is a description attached to the timestamp. Yes, okay. Okay. Yes,

Speaker or that or the or the description is tagged with the time and then that becomes you can you cant touch that anymore. knows that's already It's like a submitted and then you would but that would be only like for collaborators because it's very good that we're talking because there's a lot of things that we haven't considered that you're, you know, you and your students are going to notice.It's very interesting because I was also thinking right now, we don't want to accidentally delete stuff and I'm not sure if if we can accidentally delete something I guess not from which coffee from your local coffee or from the mouse, you delete something wrong and you update to me, you're gonna get it back. Well, not miss it live from my Well, that's sure if I'm syncing with you, you're the master. So all you have to copy is your push down to me. Because it wouldn't matter. Yeah, but the circle circuits and everything need to… Worst case, worst case, then, then worst case, we could probably not even not have collaborators maybe.

Speaker Elsa But as I like your idea, my point is you mentioned about individual accountability, the collaborative you under document who you collaborate with, and then as the lead, let's say, when we write documentation, different people include different level of granularity of details. So what if I put in less detail because I thought this step was understood. And without that accountability, you cant really go back to me to leave Yeah, well, we all know this group of analysts worked on this but individually who actually worked
on this,

Speaker how does how does word work? Or in like Google Google, right, so we would collaborate on a document. I have history who entered what, right. I wonder how that works.

Speaker Elsa Right now and so my students are using Google Docs to do online collaboration. So I'm able to pull out all the different versions that they have saved. And there is color code to show me Oh, this individual has done XY and Z. But I have read posts where when you legit say, there's this paragraph, I originally wrote it, but you came in and they you we talked with just assume that we talked and then you took the entire paragraph and you put a new paragraph. If you only show that you as the author of that paragraph, there were some discussion online about that I follow.

Speaker So I wonder if something like that. So collaborator,

Speaker Elsa so to track all the history, but what is important to you guys, if two people collaborate, they're not going to override so I'm assuming you're collaborating. So I'm working with you on this particular finding. We will Talk about all this stuff is not useful anymore will remove it. So why is there a need to store the history?

Speaker There's not, there's not I'm just saying, I wonder how are you going to do that? If, if maybe we can get away with not even time stamping it and just saying, I want to collaborate, I'm just gonna add my name to this whole thing and we both can update it. But now we have two copies of the same findings.

Speaker And what I'm saying what we've done the event is after we have two copies, we always have to sync

Speaker Elsa which one you're going to sync?

Speaker because we have one on my stuff, and then we have another copy with my stuff. So we can say what we usually do is we start numbering those findings that way,in our scheme, the problem here is merging. Right How do we merge and right now that we're doing is the way we merge it's like okay, you got it okay money, raise money for policy one with the same idea, whatever that will log on I sync to the to the lead. It gets updated when you sync it will say, Oh, no, you already have that.

Speaker Elsa See the whole idea of merging, let's just say, instead of one of us typing out the content of the finding, you create a find if you document all the steps that you have taken to get to whatever, I might have stopped already, or I might continue to do and so then we're growing our findings. Even if the system allowed us to merge, what exactly are you merging? Are you describing all the texts that I've typed of all the text you have typed and just put it into one big block? But what does that mean by merging? What are you what do you actually merging? Because it's not like the steps are, I guess labeled say, Oh yeah, I already have this. The old We could do is just do text matching if this piece of text here already this piece of Texas here then we don't merge at every differences and we'll just put it in one file

Speaker because you know that gets hairy because you have two people collaborate and you say, Well this person that this but this person did this, but he does something different. So when you put it all together

Recording 2

Speaker 0:02 Yeah, like I said over here, there's really no merging the merging that it's doing. It's just saying, okay, here's some information under description. Oh, there's some stuff there already. Okay, let me just put a new timestamp and put it on top. And that could be, this could be the same paragraph as this one, except it's always updated. And so now you have to, but I mean, that's minimal the times you do that, I guess. That might not be something that we worry about.

Speaker 0:32 And how many findings could a task but let's forget about task. For now let's just we have only task and findings. How many findings could you have for tasks you could have unlimited right? So then if in the case where we're collaborating, but you and I are trying different steps, we document it in a finding of our own when we sync it to the lead. My finding was going to have a different ID for example, than yours. So if we think both ways you want have all findings,

Speaker 1:01 and that's what happens or not. Right, right?

Speaker 1:02 And then is are there any issues with having two findings? Like, like, in our case, we're working in solving the same issues. You and I took different approaches or just documented, and that will push it to you and you as a lead. What do you do with those two?

Speaker 1:17 If I see, when I look at the findings, I consolidate. There's a lot of events where we're going to say, Okay, these six findings, they all fall under this umbrella. So, when we present them, sometimes, we just put one role that says, you know, whatever, vulnerable TFTP or whatever. And then we say it affects all the systems instead of having six different ones and say : vulnerable TFTP from system one, vulnerable TFTP system two, and like that

Speaker 1:53 So then, so let's just say those two findings are similar, but not the same. The same system because we were solving the same task. What do you do when you get those findings?

Speaker 2:07 So if they're similar, but not the same, that's two findings.

Speaker 2:10 So, you just leave it as two findings findings to the same system.

Speaker 2:15 So, then for collaborators when we push findings we'll just push it to you. So I push mine and when he is done with his he pushes to you, when I sync with you again that I will see his finding there will just be two findings.

Speaker 2:30 So the the syncing back should not be automatic, the lead would manage that. And you as an analyst, you shouldn't worry about merging, the lead does that.

Speaker 2:47 So that in in that case, we both sync with you. So what I come back to you and you push your data, either you push it all or you push nothing, there's no in between that you could allow me to see only finding A and C, but not B right.

Speaker 3:02 Okay, so what I do, what we do is I'll tell you, Hey, you know, what can you delete items two and three? Findings two and three? Because I made some changes and I want you to have the latest

Speaker 3:14 but then if you're pushing it to me wouldn't I just take it? why do I need to delete mine first?

Speaker 3:21 because it depends. Let's say that you're finding his tasks and your findings right? And you have some

Speaker 3:31 Let's say you deleted, and then you send it back to her. Then why should she delete it?

Speaker 3:39 Because if I try to send it back to you now …

Speaker 3:41 See what I'm saying? Won't her stuff get overwritten?

Speaker 3:46 Or so right now, right now it doesn't. It just says oh, I already have that finding.

Speaker 3:53 And when you say you have the same finding, you're just checking this finding ID right?. Okay. Okay, so you had deleted it. And you push it back to me. Because you don't want me to have my findings. So next time when I sync with you, you won't get those two findings while you're asking me to delete them

Speaker 4:14 I'm actually I want to say improve improving, but maybe putting the write up or adding more information to your finding and I want you to have that.

Speaker 4:29 So then the finding that you'll be pushing it to me with the same ID?

Speaker 4:35 that's a good question

Speaker 4:38 Because you won't have unless I have synced with you. So more likely I synced with you before and after. So you had a copy of mine and then you made an update on it. You want to push it back to me. When you push from maybe that's why you have the lead because the lead pushes and the analyst just takes it. Yeah, because otherwise there is no difference between analysts. with each other versus the lead syncing with the analysts, unless you guys want the extra step to confirm all you sure you want to delete it, because that's as the lead, assuming that you have the latest and you push it down when you push it down automatically overwrite anything with the same idea, I guess.

Speaker 5:16 Yeah, I guess the reality is when whatever makes the leads life easier. Because like, like, for instance, if I want to spend a lot of time going through all that stuff, and yeah.

Speaker 5:29 So yeah, so we have a system right now. That maps the network, we get these icons. Oh, we've got 10 servers and Windows machines. And we save that and give it a name right. Now when if I'm the leader, I'm managing this. I want to make sure that mindmap has my initials or something. So that when you there, because the only thing differentiating is the file name. So the other thing finally was mine, you send it out here, one of the things from happening to you, and I'm going to take on more than likely is gonna over write it. So, so what we do is I take a break now with away, I take three copies of your maps, and then I import them into my maps with a different name, right. So in FRIC, I'm thinking, if you have an IP, the finding, I just, I knew it would have recreated if there's any change, right?

Speaker 6:31 Well, if because if it was the same finding, but there's just an update, then you're going to start having multiple copies of the same findings. It will get even more confusing.

Speaker 6:51 Or would it be maybe just something like a little notification of data and this at this time.

Speaker 6:58 I think that We're talking about what are the attributes we need to care about for a finding. So time is very important. And maybe later on we could come up with other properties to help the lead to differentiate, but always in agreement that there is really a difference between the lead and the analysts are so thinking goes so efforts push from the lead to the analysts. The lead would whatever the lead that's pushing down overwrites what the analysts have and then when the analysts push back to the lead, you would just take everything. Well, you should notify us of the option to say no [inaudible], I'm not going to take this deal. So do you want to either take it all or you can select

Speaker 7:46 Cause right now we'll just take it off. But I mean, I hate to lose data and I think that's a nice thing about frequenting. You don't lose data, you could duplicate things and then you'd have to erase

Speaker 8:05 But even then when you have duplicate data, then you go spend time trying to clean it out

Speaker 8:10 to see who was, which is the final that is complete. Which of the events that I have been. Since the findings are not like our training is very easy for us to have

Speaker 8:27 I guess I guess, would it what would it be good to say that the analysts that you want the analyst maybe to have a history of their own work? That way whenever you're pushing stuff is being like pushed to you, at least you have like a history of what you did not necessarily be that way. You don't really lose a day and deleting the data is still there, but it's just that's like being pushed to the to the master of the leader. I don't know if that makes sense?

Speaker 9:00 Then I, as an analyst, every time I do something, the system records a transaction. So the one I try to push it to the lead, and let's just say the lead, say, Now I don't want, I don't want this, I still also have a copy because I'm not gonna delete my work

Speaker 9:24 That way if the lead, like overwrites something or someone adds something to it, that he wants to be just pushing on whatever.

Speaker 9:29 If data redundancy is important, and you don't want to lose data. So what if when the lead is pushing back to the analysts? Why don't we system just because, again, the ID is the same, but just so we're talking about finding one and finding one. Because it's coming from the lead, it's automatically override it instead of overriding Why don't just archive the other one, and then have the new one, you always have the history of you every restore

Speaker 9:54 and that's what we do in the current tool actually, in. This one takes a snapshot every like five minutes. Just kind of auto saves the copy. So, yeah, that would be, that would be awesome.

Speaker 10:12 Yeah, so then there will be no deletion on the analyst part. And in case after a while, we sat down and talked about the finding and your realized while the updated one is actually not as good as the original one. And when I that's why I was saying when I push back, yes, it's good that you have multiple you have all the data but after a while, it gets confusing. So then you could pick and choose which one. So then you as a lead what I'm pushing back to you. Do you want all you want to have the option to select?

Speaker 10:43 I mean, I can see both ways, I can see that the option to select would be nice. So that I can not clutter what I have right now.

Speaker 10:56 But they for that particular method, you also have the option to just take it all, So it's not either or. So it's either method number one, you either take it all or nothing. Option number two, you have the choice and one of the choices to select all. I think that's what we're doing with the system the software tool is working

Speaker 11:18 It would be like one of those. Are you sure you want to close this? You know, just to make sure that hey, why am I getting 100? Finally, see what happened here? Yeah. And get them correct my current setup or something? Yeah. I was just worried about having to have one more step to accept the data. But

Speaker 11:38 I think the when the when it come time, when the teams are doing the prototyping, I think that will walk you guys through the process a lot more because it's visual. So you could say, Hey, I play the role of the lead analysts. Let's see how many steps it will take for me to actually accept a finding from an analyst. At that par I don't know. You know what this idea sounded good before but like After we walk through it, like using some sort of a sketch, it's clear to us I know this is not effective for us, and then we'll just scrap it. So we'll go back to the model.

Speaker 11:38 Okay. Let's see. Okay, so we stopped at number 22. So in class, we talked a little bit about the notification, I think 22 is on top of the lead receiving a notification saying certain tasks are overdue. Should the analyst or the lead analyst also be notified when a task is complete?

Speaker 12:42 That would really help, that would be really nice. Having a little notification, saying hey, you know, just a little, Hey, I completed this task or something. So I saw I saw I saw this it's called gratis, a commercial tool, It's kind of like similar to a ticketing. And so you have a task. And then you grab, you have the test reflection, and you read the whole test in the sandbox that it's you're working on in progress, and then automatically the lead can go there. Now see, if you look at notification and see that this person is now there. So you have that view, you can see what everybody is

Speaker 13:26 also not only at like all the tasks or the entire events, you could see per person, how many task has been completed, how many? Is this something do you guys want?

Speaker 13:38 I was thinking through the search button system, if you want to search on the findings, to see who has done what.

Speaker 13:54 because a task could have subtasks I don't know if that's the view that you You guys should be interested in so not only seeing who is working on what But hey, I have this task, right have 20 sub tasks, how many of sub tasks are are completed? Or how many armed? Is that revealed? As you guys will be interested in?

Speaker 14:15 That? Yes, that would be really awesome.

Speaker 14:20 Okay, so then when we talk about notification, as far as progress completion goes, we have three views, we have even view event as a whole, how many of the tasks are completed. So if we look into the event view, the amount of detail is being shown us only at the task level. So if you click on a particular task, you could see how many sub task and and you also want to see per analysts.

Speaker 14:46 And like I said, one of the main things for that is to make sure that they're doing something. Or t5hey're just, they just got tunnel vision and just focusing way too much on one particular writers.

Speaker 15:05 Let's see. So how is the priority being assigned? I think what the teams are asking, is I already like one to five, where's the high medium low

Speaker 15:23 is priority only associated with task or is also associated with sub task and finding some, not more findings probably not a priority.

Speaker 15:35 I would say only for task

Speaker 15:46 I think I think if you have some tasks to do some tasks, very important. I think a subtask should have a priority too.

Speaker 15:55 We kind of talked about subtask So we want the subtask to have a priority

Speaker 16:02 if you have five sub tasks and one subtas is so important that you want to give it more priority and I might as well just make it a task that itself

Speaker 16:12 upgraded to a task instead of having priorities on the subtasks

Speaker 16:22 Okay, so priority is only associated with task and if one of the sub tasks under a task is very important, then you just upgrade it to become a task

Speaker 16:36 because I mean can you think or scenario can think of something like for you wanna prioritize a subtask? Let's say I want to scan this is network. Let's go with these linux computers to make you want to I don't know Well analysis of the servers that you found, of course, the sub task, you will go into the priority based on which of those web servers has the highest impact on the mission. And then you can save the copy. Spend more time analyzing the web server that is more important than number two. Who's going to be doing that? Not the lead right now. Yeah, no, that will be a priority that the analyst will set up for their own work. So it would be like a little more of a tool for you

Speaker 17:30 to say like, Oh, I need to do this web scanning, but I'm gonna follow this Probably the lead

Speaker 17:41 character in the lead is very low, he's going to be like, yeah, do to the web scanning. But I want you to prioritize At least your your priority or the interest for that list.

Speaker 17:51 Yeah. I mean, I could see how, as an analyst, that would be something to organize So something else, look at the task and I know how to do it. Let me just look at these 5 sub task. And this is the priority that I'm executing all the order.

Speaker 18:13 As far as, as far as priority levels.

Speaker 18:18 let me ask you sort of what this priority actually mean, because it sounds like at the subtasks level, it's just a way for the analyst to organize what I'm going to do first, not necessarily the upper management is saying that, hey, this particular task, because at the task level, it means something different as a Hey, you want majority of resource on this, that's why you're putting a higher priority. So while we're using it, at least based on what I heard, it seemed like the definition of priority changes if we're at the task level versus the sub task level.

Speaker 18:55 Priority is set by the lead and at the sub task level, it could be setup by the lead, most likely is going to be set up by the analyst

Speaker 19:07 To organize myself with the so there's so then from the very from the very typical, we would put my system from the lead as the lead system and then you tag your system as an analyst, to give them different permissions or whatever.

Speaker 19:28 for example, what I want to avoid is kind of different versions, so everything is the same and any system can be the master or

Speaker 19:44 no, but the system would be built in a way that you could change roles. So, so it's not like the lead is going to see a completely different set of interface. The interface is exactly the same some of the features again, so, let's say

Recording 3

Elsa 0:00 We make a requirement, the only the lead could assign priority. If I didn't Mark myself as the lead again, there's a trust between so let's say you mark yourself as the lead, then none of us should check that box either where the lead then by that time the system knows I'm playing the role of an analyst for this particular assessment, then I can change the priority that the lead has set, but I could set the sub task if for another event, I am playing the role delete I just checked a box I believe that I could do certain things so that the analys, what is the rule then? The lead, so a priority at the task level should only be set by the lead?

speaker 0:48 Yeah. But so

speaker 0:53 but then it kind of goes away from the from, like, if you want to elevate something like a sub task to a task We have to give the way for the leaders Hey, this has higher priority?

Elsa 1:08 well also if we upgrade a sub task to task, assuming the analysts could do so. Because I'm not the lead so I can change your priority now because it's a task. I don't know that's a good point.

speaker 1:30 I mean, I want to say that I want to say yes, but then it's in time. I want to say I want to I want to be able to give that indeed, that flexibility to say you know what, your, here are 30 tasks, it you know, pick 10 pick 10 pick 10 and then you guys prioritize, based on what you see and some little work like that because I really know nothing about the system. You guys have much brain soreness, and So,

Elsa 2:01 so then the priority is not really is it just and what order you should get things done? Not like one task is really more important than the other is that Am I understanding that right with the

speaker 2:14 flexible but

speaker 2:15 yeah, so so as a leader, you want to make sure that we accomplish a minimum set of things. And so those are things are going to have a higher priority. Okay, well, you gotta, you gotta do this, that's for sure. If we don't do nothing else, and then we have another list of as time permits.

Elsa 2:38 So then I see the importance of the lead, only the lead could set the priority.

speaker 2:45 Yes, yes,

Elsa 2:46 because you have control over all the tasks pertaining that what happened in this event, if you start letting the analysts said it, then at the end of the event, Let's just say, none of the analysts, let's just assume in the extreme case, none of the analysts marketing and critical, then they could be doing even more of a minimal amount compared to what you guys have planned. Yeah.

speaker 3:15 So I'm gonna take a step back, it kind of brought something appropriate just to kind of like for me, it's easier for me to visualize. So so when we now go into a test event, I want to say so as far as when we talk about well the leads can assign tasks. So for me, it's going to be scanning enumeration is gonna be a task. Documentation review is going to be another task. Maybe packet sniffing is gonna be a third task. So within your sub task and a half, okay, so I'm going to scan the numeration report in that nessus game. I'm gonna do like, like a website. So let's say if I were to identify vulnerable, vulnerable j boss within the webcam, and I wanna say, you know what, I want to take this and I want to make this into another task in itself. Why? Because I'm often Someone actually focused on this actual vulnerability. So I guess this will get promoted to a task, and so on and see right now, everything is kind of being independent of each other. So I can get one person to do documentation a person do packet sniffing. So once like, for instance, once this guy gets populated these two items, land map, and this is especially now here and start to my collaboration, I can say, Hey, guys, here's the network. Here's the the vulnerability, the vulnerability, excuse me, vulnerability scans of the system. So and then like from there, we can kind of go in Okay, so the scanner also identified that they have open NFS shares, so 911 for one person to functionally focus that he wants you to connect to these NFS shares. Do I guess it's a parcel of the data and see we can find any credentials or anything that's valuable, and so forth. So that's how I can help I kind of see the whole subtasks I'm not sure if you remember, or me that kind of makes me kind of makes it easier to see visually. I don't know, this is something that maybe we should kind of like, like tell your students like,

Elsa 5:13 yeah, I think providing examples because at this point, I'm so a little unsure what exactly is the difference between a task and a sub task based on business out like tasks like a theme, right? And the sub tasks are actually steps like instructions. So the analysts do this, do this and do this. And as a result of doing this, if I could find a vulnerability and exploit it, then I attach it as a finding. That's the at least based on the discussion. That's how I'm understanding the differences between tasks of tasks and findings with the idea of promoting So the example that you mentioned about oh, this is a finding and then you want someone else to focus on this task. Why would you be creating this sub task? Shouldn't this be created as a task from the beginning? This has my come later Well,

speaker 6:00 what was the scene? What have you seen? I mean, here's, here's the problem. I mean, every system is different, every network is different. So essentially, we do have a script of things that we want to run it first. Why? Because we don't know what's on the system. And not only that, maybe from, let's say, the Steelers, the army translated every year, we're scanning a brigade. And we're scanning the company for a division. There might be a cases where that same issue exists in all three echelons. But or it might be that is only exists in one. So we don't know that until we scan. So that's why I like like, for me, when we go into an event, I want to make sure have people started with the scan documentation. And you see like for here, what when we get to the webcam identifies a j boss vulnerability. So I would like to have that as a task. So now that I know that I know that that Jay boss vulnerability might potentially exist within That net within that network or that Echelon, then I want to make that into a testimony of someone focused on it. So, if they were actually once they start focusing on this particular task, they say they actually exploit this. So if they exploit this then this becomes a fine you know, so I mean it may not be under this guy but at least it's defining is being attached to this j boss chief issue. Yeah. So see them finding issue to the whole finding work gives me headaches every now and then. So I call it a J boss issue that invites them to a boss session. So once I confirm that I can explain it in a in one that's an actual that's a true fine.

Elsa 7:46 That's why in class I was asking, based on the description It sounded like so in the current system that you guys are using might not have those concepts in place. Since we are building another one from scratch. If is necessary to introduce another layer to help you guys organize your, the data that you guys are collecting, I don't see any reasons and not doing so instead of having maybe like two types of fighters, so, finding with a property is is really a true finding or some really ambition right.

speaker 8:26 So, you get my spiel now.

Speaker 8:31 So So essentially what I was saying is that like if you like, initially we're going to test we have we already know, there are certain tests that will be removed for instance, task a would be scanning and enumeration or task B would be like a look at the documentation, make sure that we are doing what we need to do. We had the blacklist, the white list, and so forth, the IPS, whatever, blah, blah. And also then we will have like, let's say we'll have one person Okay, so, these guys are standing. So this is the This individual or maybe these two individuals are scanning team. So So go ahead and start sniffing the wire. Go in there, see if you can find anything, maybe there's maybe there's some credentials that are being passed in the clear text, or whatnot. So so then like, under, let's say, under understanding numeration, your subtasks would be n map neces and running a web scanner. And what I was saying is that what if the web scanner identifies that there's an issue with Jay boss, then essentially, Jay boss should be kind of promoted to a, a task itself? Why because I want to, I want to have someone focus on on that Jay boss Jay Jay issue, and then once they focused on that Jay boss issue so they actually find that they're able to exploit it and essentially, the word gets exploited gets populated as a fine. So that's, uh, that's kind of the process that I see them, but I see that I see that working

speaker 9:58 but and so under that constructives, and subtests, don't get, don't get prioritized?

speaker 10:09 They get promoted, you get promoted. To me, I would say that they would get promoted to a task. Yeah. Because the reality is that when we go to assessments, we usually have one person, or maybe two people that most that are actually scanning. Why? Because if we have, if we have a team, let's say we have a team of five. And then let's say, well, let's say all of us where we're starting to scan, essentially what we're going to do, we're going to we're going to create, we're going to add a lot of congestion to the network. And so congestion is latency. So it can be like a you know, it might be issues getting some of the data back, we might have some discrepancies because you might lose packets or whatnot. So that's one of the things that we want to avoid is is is having a lot of contrition. And also because if you have if you have one system that's being scattered Bye bye for other systems, the more likely you're going to, you're going to create some type of denial of service on that particular system because it won't be able to handle all the all the incoming packets and so forth. So that's one of the issues. Well, that's one of the reasons why we want to have at least one individual person or at least to scan and just because this these people identify certain issues when when, when the number doesn't mean like, hey, the people that are scanning I mean, you're already scanning your you might be reading some other scans or whatnot, so it's likely that someone else is not doing anything. Start workong on that, on that Jay Boss so essentially you work on that task.

speaker 11:40 And and going back to the question of priority, I don't know if it would be low, medium high. One, two, three.

speaker 11:52 I guess if we were to do that, we probably need to give them like a rank some type of ranking system. I mean, if we do, high, medium, low. I mean, if you do high we'll say you're going to be able to get a credentials. Let me know probably something that's something that needs to actual act well, I guess I should say actual access to the system. We can do something like where we can find hashes. But I don't know that's a that'll be like a high priority. Why? Because the likelihood of you actually cracking mustaches, I mean, essentially standard low. So

speaker 12:29 So, so you have to think for the priorities, we would have like three different types of priorities. Or maybe turn that to students and have them recommend something?

Elsa 12:43 So there are some things that they could go off and do the research this really need some, they need the domain knowledge in order to be able to even recommend this one. I think it's better if it's coming from you. So right now For

speaker 13:01
Let me make a note here to define it.

Elsa 13:05 And then so the lead should be the one to set priorities where everybody could everybody can separate. Okay. And then it's only at the task level. Right. Okay.

speaker 13:15 And it could, I mean, in fact, I didn't make that on that. When we were doing the briefing, the one that has tests and then tasks and yeah. So this guy is can, so see how this one can take. So is when you can input JPEGs artifacts, even for the tasks might be good to, you know, be able to maybe take like an IP list like some type of text document even if it's just information. Something that we could, you know, that would even matter. Because if we could just copy paste, well, now I can do a task and say, Okay, I want you to scan the systems. And here's a PDF with the architecture in the documents. And so I could put artifacts as part of the task.

Elsa 14:18 Okay, so then task. So the attachment as really extra information that would help the analysts do their job, but not as evidence. If we have so we have attachments to a finding and attachment to a task. of Do we have attachment to subtask going by that logic that you mentioned, we should, because those are additional information for your analysts to use.

speaker 14:48 Look at this file. Go through, go through this is all we get or let's say we must say the task is to login NFS we found and then the sub task is to look for password files. And then we end up getting another file shows interconnections between systems. And then on that same kind of person, we could get a subtask and say, Hey, you know what, we found this file on Shirou subtask. I want you to look at all those machines and see if there's, if you're able to log in. So be a subtask. With with additional information.

Elsa 15:34 So at all levels, you'll have the ability to attach an attachment. Yeah. The meaning of the attachment changes not technically attachment as an attachment in the eye of the system, but then attachments and a Tesla from a subtask they are really instructions for their instructions. Yeah, yeah. Okay.

speaker 15:56 Finding it's like evidence.

Elsa 16:02 So, one issues that I have heard from I think it's from Vince different people are using the system a little differently, and they're interpreting different fields differently. Now that we're talking about maybe standardizing some of the process and some of the information being collected, would it actually make sense to rename instead of just an attachment, give it a meaningful name at a finding level here, really, those are the attachment pies where the evidence of attaching and then for tasks and subtasks really attaching supporting material

speaker 17:00 Listen to this is for a software project that we're doing and we're just one probably requirements. .

Elsa 17:19 So we're in agreement for task we're naming a good quote unquote attachment to supplementary material. Yes. Okay. Same thing with subtasks supplementary material and for finding the attachment is really renamed as evidence. Okay, so let's just move on to the 24. Will our system be interfacing with any systems where we could gather information about the event tasks where everything is manually being input by the analysts and lead analyst manually input?

speaker 17:54 Unless you want to suggest just like a test plan or something like that, pre populate those. I don't think....

Elsa 18:07 So manually?

speaker 18:09 and again, the only thing is, is, like I said, if you put document or documents or whatever on a certain task that's it for for supporting the information.

Elsa 18:21 Let's see 25 should the system alerts the non lead analysts if the task their sub task is linked is complete If yes, please elaborate on the preferred mechanism. So I think what the students are asking is, if I have a sub task like completed it, with the analyst actually be notified.

speaker 18:44 The analysts or other analysts?

Elsa 18:47 it's unclear should .... be complete ...Move on from this. 26 Should the system allow the lead analyst to swap tasks? So let's say I was assigned this and then I want to give it to you. Could I swap it? Well, I don't think they're talking about collaboration or passcode. Capacity on the task.

speaker 19:16 Yeah, yes, definitely. Yeah. Because that will happen all the time.

Elsa 19:19 Oh they do swap?

speaker 19:20 Yeah. But let's say, I gave you 10 tests and 10 tests and 10 test. But by Wednesday,

speaker 19:26 Let's say I'm done with mine. He can start moving some of the stuff to mine because his was hard.

speaker 19:30 This was a lot of stuff, or didn't have anything new. You're just haven't had a lot of stuff and you're barely testing. So then we gotta reassign some of some of your classical. So then how does it actually work? So I guess on day one, when we sync with you, you gave us our assignment you have 10. 10 and 10. I only finish let's just say three of them and you completed yours already. You would have synced with the lead already.

Recording 4

Elsa 0:00 all of yours is complete, all of this will be required to sync with the lead. And then we re and then

Speaker 0:06 yeah, ideally, ideally, I'm going to do the change, right? I'm going to change it. And I said, Okay, I'm going to change the, the, those tests, and then I'm going to push back and the view the updated. Maybe, maybe that's a

Speaker 0:20 but you also want to give the users?

Speaker 0:22 Yes. Oh, yeah, definitely, definitely. Or I can just say, you know, what, just go ahead and get three sub test three, or test three go ahead and assign to shuffle, or Elsa I just kept get out of that task. And even though, even though it doesn't matter what I have here, next time I get it. I'm going to get task three with him attached, right? And I'm going to have that little check that says, hey, do you want to adjust everything or just these?

Elsa 0:48 So you would have, so if let's just say for some reason, you got Call away and you are meeting with the customer. And so I'm not done. You're done already. We talked internally and so I How do I actually so other analysts to analyst level, how do I turn off myself as

Speaker 1:07 maybe when um maybe when he tries to sync to you, you just get a Hey, there's a little collision here. Accept the change override or

Elsa 1:19 but isn't it very risky just to swap the task to do a sink like that?

Speaker 1:24 But the way works right now like I get everything so I'll tell them hey you know, I'm going to help you with task number five. But everything I'll work on it, and then label it with my initials. Cool. I wasn't one to work on it. So whenever we sync to mine

Elsa 1:39 But but so in your case, you would have changed but just forget about subtasks for now. So you have changed the task being assigned to you. Okay. So then if let's just say you synced with Juan first before Angel syncs with Juan, then how is, let's say if you left them out of the loop, you got a call from the customer and then we both synced right

Speaker 2:05 I sync the first and he syncs the second, but the way it works when he gets both of them okay or task. My queues will be empty because it doesn't work. Mine will have notes. So in this case it will erase

Speaker 2:23
Yeah. So instead of replacing or anything, I make the decision of what to take

Speaker 2:27 And the way it is working right now, we since the system cannot account for that we usually start labeling like the task or the findings a way that that he knows whether it works or not

Elsa 2:40 So then ideally, how would you want it? How would you want the system to handle this?

Speaker 2:46 I would like to see a timestamp on on when was the last one.

Elsa 2:52 So, again, this might be a ridiculous scenario. let’s just say, we had an agreement that you're going to work our stuff. But for some reason I forgot to hit the Save button until five hours from the time when we made the agreement. So then when we tried to sync it if we're just going to go out a timestamp my I'm going to have a later time than yours. That the system or even like just say the lead was left out of the loop. He has no way and telling the other than looking at kind of, what if I had done some part in it and the lead might

Speaker 3:22 Yeah, that's why it doesn’t matter. And like

Speaker 3:26 See that’s why you guys are good.

Elsa 3:33 So how about we do to follow as far as the sinking issue, it seems like there's a number of scenarios I could turn to the class and have them you know, what, have some teams might actually write it down and then I could have a discussion with the class and see what are the pros and cons with different ways of doing it and then we'll come back to you and propose, hey, based on what we heard from you guys, this is what our analysis shows

Speaker 3:59 We don’t want to lose anything we rather duplicate data and go through it manually? Because it is not like constant constant.

Speaker 4:07 Especially because it’s the findings and I mean, usually, for a big event I mean, for the most findings that I've seen, I mean, there on the teams 20 to 30.

Speaker 4:22 It's usually more like six to 15. so it's very manageable.

Speaker 4:29 Sooner or later, even though they take away the lead. He comes back and the worst thing, you know, we can sync up and say,

Speaker 4:39 Yeah, now a task a task can be,

Speaker 4:41 yeah, that is hundreds.

Speaker 4:43 Maybe not, but it could that that that could be a lot of stuff. Especially once you have like 10 people, imagine 10 doing 15-20 things, you get into the hundreds very fast.

Elsa 4:56 So therefore the tasks does the lead sets it up or when the analyst creates it, everybody could have right access and update attacks. So even if analysts thinking I didn't create let’s just say, or you created a task, and I synced with you, and so of course, I have a copy of yours, but I didn't create it. Should I have write access to yours.

Speaker 5:16 I personally would like to see that, but I don't know how to another, you have my description. So I don't if to go and update the description, or just to add to it to say, Hey, I will keep it. Also, keep in mind that, you know, this also affected this other systems or whatever, instead of replacing what you already wrote. Because it's kind of what we do. Right now we have in that other system we were talking about. We have this notes tab for you go and you write what you did when you timestamp it, and then you write your note. And you can mess with that. And then you want to write another note. You time stamp it again and then you write another note So it's always depending on the notes. So So I would say, yes, have write access, everybody could have write access

Elsa 6:00 See, because in the RDD right now, if you did not create that task, you can do anything. I think what Vince added was at finding level. I don't remember as of a result of our discussion, could you actually update the task? I think her radio was saying the one she went for the assessment, she could update a task, but then when Vince went for his assessment he couldn't it depends on the lead to see what you could do

Speaker 6:31 I mean, it's, it would be nice to be able to do both. But how do you accomplish that sentence? We can accomplish this very easily by doing an operate and operational

Speaker 6:46
Or its we just talk about it or we set the rules, but to do technical control, and that you have to implement kind of roles you would have to implement roles and say, okay, say you roles as analyst for this event. Or say you roll that, right? So.

Speaker 7:06 There's some type of requirement where we say, so we say, hey, so if you're if you're the lead, you're going to be able to config you need to configure how you want to do it. So let's say we want to give a, if you're the lead, you want to let people override and say yes, the moment right. You don't want them to do that, then you can do that. I mean, that all goes back to someone, excuse me configuration, like I say, hey, so sync to this person sync to this person, or what not, but

Elsa 7:39 we could look into it. And the lead for that particular event will set up all the rules. And for that particular assessment, those are the rules that everybody follows. And then the lead has I guess liberty to change it,

speaker 7:54 The new configuration for and you can say hey as the lead. That's where you can assign your task. You can say hey I want to make sure that these five tasks get done first and this person will do this and this person will do that or maybe just leave it up and just say at least define your initial path for that, and go from

Elsa 8:15 there. Because there's a system that I saw doors, I have the super user role. So I could create accounts, I could create a number of things. And when I create the accounts for the students, I have them as the author role, so they could change big ad like like traces and they could add notes to it, but they cannot like create a new project. So we could do something similar. So there's a config. Before you guys start the event, delete would have to set up those rules based on a number of criteria. Once that is set up for the entire event, those are the rules. Everybody goes by. Yeah, okay. Um, let's see so 27. Which aspects of the task are editable after initial submission? Or does it not matter?

Speaker 9:06 I would say. I will say everything is editable

Elsa 9:09 Again, going back to what we just agreed on is really depend on what's being said in the configuration. So 28 after an event is finalized, is it possible to edit the event, the tasks and sub tasks associated with it? So then how does it work in this particular system? So other systems we have worked on once you complete the assessment, you swap out hard drive, the data from one assessment is not going to appear in the other

Speaker 9:40 Essentially the data gets reimaged

Speaker 9:42 But data kind of gets kind of synchronized to one drive or archive and the rest of the drives is testing

Elsa 9:49 But then you will have an archive copy.

Speaker 9:51 Yeah, right. So essentially, I guess this is the way we do it. We do it in the way we do it and it works so. We have a test. We think everything. So everyone has a copy. So once the lead has his master copy, once they go back the other drives essentially go back to the hard drive for the mega reimage. The leads copy essentially gets the data from there it gets uploaded to another system. So essentially it's the what's it called the

Speaker 10:23 The one that robs me, Intel bucket

Elsa 10:29 You achieve it and then you move on

Speaker 10:33 We do the same event. Lead usually pulls and review what goes on.

Elsa 10:38 So then the system should also have the ability to reopen the event.

Speaker 10:45 That would be Yeah. You know what we are going to do the same tasks we did last time, we might add these. That would be ideal

Elsa 10:53 See, because in Google Classroom, there's a feature called a reduce. So I have 3 Classrooms and some of the tasks there are the same. I will just create one post and attach whatever as attachments are required. And then for the next classroom, I just say instead of creating a new post and type everything from scratch, I reuse it. Yeah, I like that. So we are supporting the idea of opening an existing event.

Speaker 11:25 That would be nice that that was especially like, I'm thinking like, aqua, and SONDA, or if their events that we do over and over and over, it's the same event that we do the same procedures, everything and every time that we do it, we have more experience, but we reinvent the wheel again from scratch. We start doing everything from scratch

Speaker 11:48 I mean not only that it will help us out with the verification of fixes, so the waifs we do so essentially, more than likely after a certain a certain time from us was like about a month or whatever, after they get the report then the customer usually call us back to do the verification to fix it. So, I mean, we don't have to reinvent the wheel and let me go straight to whatever we have

Speaker 12:12 oh these were the findings. Right. Let's use them to see if they were fixed.

Elsa 12:16 So then when we talk about reopening and existing, so opening an existing event, you could go back and treat this so use it as sort of a template with all the findings all the tasks and but you rename it as a different event

Speaker 12:28 Yes I would classify as kind of like the like duplicate, duplicate, duplicate and call it now BOF or call it now event

Elsa 12:40 And then you could remove things that you didn't, it's not applicable. Okay. So we're supporting opening existing events just for viewing purposes, or we could duplicate the event. When you do the duplicates, that's when you could change things. Okay, so when I first open it, could I change it?

Speaker 12:56 I will say yes. Okay. And the reason for that is that sometimes. You've had to go back and see, you know what? I could have probably written that better.

Elsa 13:05 okay let me see what 29 is covered? So 30 How was progress measured

Speaker 13:19 Are you talking about like percentage wise about it? You're talking about the task itself, right? Yeah. So right now the way we have it's very again, it's very subjective. So right now, we could go for you can just pick from one to 100. And you just move the slide. So I would say the analysts has that decision. I don't know you guys. Right? Because because they're the experts. Right? The analysts are the experts. And they're the ones supporting so I don't want to tell you, oh, you're 50% done

Speaker 13:58 So so so many essentially, we can essentially do away with that and just say either in progress exactly either not started in progress or completed.

Speaker 14:12 Yeah, and that's why I brought the, the example of a ticketing system because when I submit a ticket to fix something in my system, I get the automatic. Oh, I it's been received acknowledge, oh, it's been assigned to so and so. Oh, your ticket has been picked by so and so and it's in progress. And then all your Ticket Ticket has been completed. So we just get

Elsa 14:32 So then I like the idea of assigned, I think as the lead you want to see especially if people are creating tasks or you create a bunch of tasks, but then some of them are not

Speaker 14:41 Imagine that view. Elsa, tasks assigned. task completed Angel zero. Andrea zero.

Elsa 14:58 So not started in Progress completed, do we need to say assigned?

Speaker 15:06 You know what that would be a good one. Okay, because um

Elsa 15:09 Then you could hold people accountable because if it's not assigned, then that's in the main bucket. So, those status, it's only attached to a task, right? So what if I have a task with three sub tasks? You don't have to track at the sub task level right? But then early on we were saying that we

Speaker 15:28 I thought we do at the sub task level

Speaker 15:32 So, for instance, kind of going back to my example here the scanning and enumeration, so subtask one is in that, so that can be assigned. And that's may be completed, but then you have your Nessus your Nessus sub task and that’s not assigned. So I would say yeah, you know, I like to track because why because essentially Nessus is one of the tools that we use to get the I guess get more information from the network itself. So for me, I will consider that important so I want to know if actually someone's actually scanning or actually doing

Speaker 16:09 But even after the Nessus scans some things some system will pop up and one analyst sometimes cannot do all of them, you want to be able to say like hey I don't know if I'm please help Oscar with subtask two and three because he stuck with, you know, with one.

Speaker 16:25 Yeah, but they see you not going to get to that point unless you know whether they actually started working on it

Speaker 16:29 except so then at that point, if you have a, let's say, you're going to have some tasks that are that don't have subtask, right. So if you have a task that has three subtasks, then the completion of that task is going to depend on those three subtask. So do you want to give them values now and say 33%, or, or just in progress if it's not completed, or you want any sub test to have its own no started

Speaker 16:35 I will say in progress is fine just because I want to know if someone actually if somebody actually took on that task

Speaker 17:02 For instance the in map stuff was done by let's say by the bay. You're going to tell someone hey go map the network and they started they start mapping network and that's it so but the other thing is that essentially Nessus you don't really need it but it's a good to have because it gives you a lot more information as far as a potential issues within the network that so you want to get that and then once you once you once you get the the Nessus scans then you you want to you ingest that into your invade tool essentially will populate the map and it's, it's, you know, hey uhh

Speaker 17:37 what about what about the sub task with a task? What if I take a task and it's in progress, but I'm not able to complete it because I don't know how

speaker 17:49 or I can't complete it.

Elsa 17:50 You should have another status say

Speaker 17:53 transfer to or ready to transfer

speaker 17:56 or uhh

speaker 17:57 help needed

speaker 18:01 Release. You should be able to release that. I mean, not that it's going to prevent anybody from taking it over. But what would you do?

Speaker 18:11 I think the way it works now you ask for help and somebody comes and helps you out. And then you just completed it

Elsa 18:21 I think the important statuses not doable, some tasks. Maybe it's just not doable, and I should count against the analyst or to the overall progress, like it was planned, and it was attempted, but it was just not doable.

Speaker 18:35 Yeah. So essentially, like you're not applicable let's say one of the subtasks is to do the web scanner, but you find that there is no web server

Elsa 18:44 Not applicable. So going back to my original question, is it just at the task and subtask

Speaker 18:51 I would say it’s at both. But I mean I don’t know. these guys know

Speaker 18:55 I want to track the progress

Elsa 18:58 I like so if all Task would have sub task, I would say no to at the task level, because the sub tasks, the aggregation of it would detect, would determine what the progress as far as the task goes

Speaker 19:12 Some of the subtasks may have a bigger weight than other ones, you know, is not like equally divided among the sub tasks. Like one subtask, maybe 60% of the whole task. While the rest of the other party will be.

Speaker 19:28 Yeah, so that's kind of in a way I would. I mean, I see the way, the way that I would think I would track the subtask would be simply by seeing that the task, that the task level is in progress. So if it's in progress, then I you know, I

Speaker 19:48 But wouldn't you want to know what's holding you back or what’s keeping you from proceeding. So, essentially, kind of going back to this example. You have you have your scanning, you have it in progress.

<u>Recording 5</u>

speaker Okay, so it's in progress. So why is it in progress in which the MMS can so you know, the Nessus is not done web scanner. Oh, that's an NA because it's not

Speaker you know what? I don't agree with him, but we need it. You know why? Because I just remembered sometimes, we have an event that's five days. And I'm like, Hey, you know what? My daughter has her last soccer game. And I can go there on Wednesday, so I'm only gonna be there. And Oscar's like, oh my god, something's falling me. So, he goes in. So that happened to us. And so, I left them to or somebody left Tuesday and then I showed up on Wednesday and I didn’t know where the heck the other guys were, and I didn't know what they had done. We didn't know remember, remember him? in us what was it called again the silences and we we spent, and we spent about two days and we doing stuff that they are. And it was it was a big, big waste of time. So yes. Once again, enjoy.

Elsa So, subtasks and task

Speaker yeah, that's because that transfer is it's it's incredible how much how much sometimes we'll be over there an administration called Hey, you need to fly out to DC and support me in this meeting I'm sending somebody else next time and so, they get in there and you spend a whole day, day half not even knowing where to start.

Elsa So, so then if a task of subtask the status the progress of a task should be impacted by the subtasks is not something that should be said, or what if I start off creating a task first and then during the while the analyst is trying to work and then you start creating sub task. So, one thing that we could do, the system should be able to be smart enough to Say, Hey, when I create a task before the analyst or the lead could change the status, you really need to take a look at if there are dependencies. If you have children, then you can't. The status the progress is really a reflection of the status of children. Let's just say I initially marked it as in progress or not started and then for some reason I heard someone talking about this particular concept as of oh no, you know what let me start of subtasks and I will still working on it. Yeah. Because there is a creation of a subtask attached to this task. And I marked the sub tasks as in progress then system automatically change the task as in progress. Okay. Okay. And then there's no progress of finding level, right?

Speaker No, essentially that's fine.

Speaker Anything that I was thinking but I don’t know if so much, it would be like confirmed vulnerabilities for informational purposes.

Speaker Oh, no go ahead. I was just gonna jump on this point. Yeah, that's that's a good point. Because you were reporter findings. It's either a vulnerability or it's something that's informational. So, I mean, if we can make that distinction on the findings.

Elsa So, do we need to create a new concept like you're saying that there is now tasks subtasks issue and findings, findings are actual vulnerabilities have been exploited issues? I Well, you kind of believe that there's something wrong in here. So, do we need to introduce a concept called issue?

Speaker Well, I mean, you don't necessarily have to guess in your findings. Maybe we can label it, or label something that says this is a vulnerability or

Speaker when we start a new finding, so we pick the new finding. When we’re going to build a new finding a new finding and then maybe the first thing is, you can confirm ability. I don’t know what else Information formational

Elsa

So, moving on to findings 31? Are the findings linked to each other under a sub task or a task? Is it correct to say the following if a task has sub tasks the findings should be attached to a sub task? If there's no existence of a subtasks in that structure, the findings are attached to a task.

Speaker But what if nothing, then it's, that's an orphan.

Elsa But what if I am starting off as a task, I found a finding then like like some of your examples here, long doing the I identified the subtasks I should have done so then Initially, I had tasks and a finding attached to the task. While I'm addressing this, I created a sub tasks under this task. So then, in other words, I could have a finding directly attached to a task, while having a sub task in the same structure?

Speaker Yea I don’t see why not

Elsa Biggest fight so my understanding is that task like a bigger picture. So, it's a big umbrella and the subtasks is a piece under that umbrella. So, should findings always attach subtask?

Speaker Yeah, I think you should be attached to a sub task. And kind of going back to this. I mean, if, like for instance, if I exploit the J boss, I'm not gonna say this is a finding other scanning remuneration, I will say so, so finding under the J box which is this subtask, I mean, if I wanted to promote this as its own task and just hey this is the task that that is the result is associated with

Elsa so when the rule is said a finding, is attached to a task, if there are no sub task, if there's an existence of a subtask finding has to attach to a sub task and the scenario that I mentioned What the analysts or the lead would have to do is actually create that so called sub task under a different task, and then you can put whatever findings. and findings, could they be linked to each other? I don't think the student asked about that. But

Speaker would they be linked to each other?

Speaker Yeah, it's possible its possible. Like, for instance, a finding could be FTP is using FTP is using anonymous as its user. So that's, that's, that's finding. But another finding would be that they're actually using FTP. Okay. So those are two different findings. One sets anonymous, but the other ones are using FTP, why? Because in the army it’s a really, really hard on clear text protocol. So essentially, that's like a field on its own and FTP falls under that, but then at the same time, you have FTP session anonymous, as as a username so I would say yeah, they can be linked to each other

Elsa So, findings linked to each other.

Speaker Yeah, one thing that I was gonna say is sometimes and depending on on the lead or depending sometimes it's a requirement from the from the system owner will have like these four findings, right? And we're five findings and then maybe these three findings affect the same type of systems so we could say hey you know what, Group them by IP so these three so now I have this system or these three findings right and then there's others that say, Oh, no, no, don't group them by by by Group them by how similar those findings are. Right? So, if it has to do with password management, and then we'll say okay, we have this umbrella over here with Password Manager, okay. So now no, let's group them with because these three management issues. does that make sense?

Speaker So, so kind of piggybacking on what Juan was saying Like, for instance, a clear text protocol. So essentially, that can be a finding on its own. And it can be clear text protocols and he’s going to say, hey, what protocols or going to take tell them and FTP? And right under that you can say hey all these systems are affected by them, but we'll Juan say and also, you might say hey, well, we have this system x, system x actually has FTP, Telling it, blah, blah, blah. So yeah, I guess that is how you group them

Elsa So, I hear two scenarios. One is three findings are for three different systems that are similar. Look, no three findings are similar for three different system. So, you just want to say hey, this finding is for three different systems. How do you actually based on the structure presented, how do you actually represent that? Because finding there's nothing underneath finding?

Speaker Yeah, so so that's

Elsa and the system is not part of a task. So, you Create tasks for different systems where you create a task unless you create a separate task. Say this task is the coverage is for 3 systems and then you put the finding that we're going to get together, pick one of them and just attach it.

Speaker We do it manually.

Speaker Yeah, because I guess how when when it's a tied to a task for subtask. How, how strong are those bonds?

Elsa in, in the system, they're just saying that this one reference this, this one reference that,

Speaker okay. Because there's been times when like for example, I remember this one time that we had to go brief, you know, somebody very high up. So, we went to the Pentagon, and we had about four or five years of findings. All the systems, they said, Okay, look at all of our different findings that you have from all the systems. And I want you to pick the top six, I want to, I want you to pick four to six buckets, where you can put all the findings in there.

Elsa So those are common findings across all system?

Speaker It's not yeah but you have to like really like for example, let's say let's, let's give an analogy of a car. Let's say your car lost air is losing air, your tires, right? Or your your tire blew up, or your tire is wearing out or your tire is dirty. And so, we say okay, tire problems, and we throw all those in there. Does that make sense? So, you will have to come up with with kind of like a like a bucket. I know don't know what else to call it, like a bucket a type of type of issue. And that happens in some events, where we have findings and then we have for information or whatever, but we have so many systems in there slightly different that we want to clump up together. And I guess if they're not tied direct, if they're not very in the bonds are not very strong, so we can just move them together and say, Okay, put all these under this. I think FRIC allows you to do the type of finding because that's gonna be important because when we click Print, or export, and we get that BRD we could, you know, potentially customize exactly how we're going to get it

Speaker Yes. So, kind of piggybacking off of that is that it? The outbreaks are usually different depending on who your briefing. Like, for instance, if its someone high level, they don't care what systems having the issue. All they want to know you're using clear text protocols. When you're when you're briefing, the techie guys. They want to know a technical knowledge exactly what was their personnel they want to know mission impact.

Elsa So, then a way to classified or to organize the findings. It's really by system. That's one way by a type of issues, I guess. Yes. And I'm guessing there isn't like a standard list. The list could grow. But But is there something to start off with? So, every time we go go out to assessment, every copy of the system would have some predefined, I guess system value. So, their system one, two, and three.

Speaker And I think that's something that we could provide, like, for instance, off the bat is clear text protocols is one category. Weak, weak passwords, or weak credentials, that's another category.

Elsa And that happens. We're tagging at the finding level, right? Okay. Yeah, that will be good. Again, this question touches on like the properties of the attributes of what we need to store per finding, if you could give to us such as a field that we add to it because once we have that field when you generate the report, then you can start doing different organization without actually having to look at the actual content of the finding that might help the lead in generating something quickly

Speaker You know, we can leverage the peak cap, at BG cap BRD's. And we did a pretty good job of classifying that.

Elsa Okay, and I'm assuming that list system will have a predefined list and I guess you can start growing again. So Frank and the other office who did some work on ontologies it will be nice that let's just say you called chocolate ice cream which is a CIC and then you spell out chocolate ice cream and then you say C. ice cream so Different people have different ways of naming and then the bike and to support this to build an ontology so that every time I mentioned chocolate ice cream all three acronyms or whatnot will show up but that I think is like the next phase but if we could solve this with a predefined list and I may be the next phase with the so growing that are from predefined list now we could add in their ontology support to allowed you guys to grow that list of the capillaries. Okay, so finding so we're in section of findings. So, if the analyst couldn't find anything, for that particular task, there will just be no findings. Finding can it have more than one author? So, we're collaborators and Okay, so collaborators. So, we already talked about associated finding to another finding. The students are interested in seeing what Data artifacts, data artifact is

Speaker for JPEGs. png, shadow filing

Elsa just attachments**,** What if one of the findings is deleted what should happened? I guess this one probably based on the analysis that the students would be doing as far as the sinking and duplicate and probably that would answer that question.

Speaker Yeah. What would happen? I guess at that point, the lead was

Speaker on the criticality.

Speaker I guess since we were going to be archiving. It could say, okay, Was this an error? Is that why it got deleted? Or do we believe it because we figured that it wasn't a finding something that happens. We're, we're we had an event when we went, and I found this really big thing on printers. And some people agreed, and other people didn't agree. And at some point, come back in there. And so, if either finding, I would say, I would say, archive it.

Speaker So so, then kind of goes back to another scenario was like so. So, this whole printer thing might be an issue, but do I really want to report it? Is it why I finding it? I mean, do I find it. I mean, I could report on the report on the actual report, but do I want to out brief this?

Speaker So maybe, so maybe when you're gonna do your ERD When you're going to click that export? You can say, Okay, let me pick the six this one.

Elsa Because I was thinking it because you guys will have a discussion to see if this is relevant or not. At that point, can't you just mark at another status and say, Hey, not relevant at this point are irrelevant and then when you generate the report then and again, having those options is good You could pick intuition. put all of them in the report or put some of them. But unless we have the tag, we can't really do this. So, shall we introduce? So, at a finding level, what would that properties be called? What type?

Speaker Leave review?

Speaker Yes, it's a good question. We'll call it but uh, you know, sometimes it's kind of hard because some, some people end up putting a lot of effort into it. And then when you tell them I don't want to out brief it or there's a consensus that you know, it's not that relevant. But yea

Elsa Relevancy on a scale from one to 10.

Speaker Maybe, maybe, out brief yes or no

Elsa out brief yes or no. I guess the naming of a particular property, we could work on it, but at least the students are aware, hey, for the finding, there's this extra property that we need to store, the naming the change of name, it's very minor.

Speaker And what that does is that it means that it's gonna, it might exclude that finding from the report,

Speaker you know, being politically correct. Call it like mission impact and then assign a number to it.

Speaker Like high medium, low,

Speaker I don’t know, one to 10 or something like that. This was territory.

Speaker So just real quick. So, if we were to say, let's say out brief level does that mean that it would exclude it from the actual report or or is it just for that.

Elsa So, there are a number of ways we could tackle this on the report page, if we're talking about the interface, we could have all the properties as options for you to select. So, if a finding needs those properties, then it would appear in the report. That's why I think maybe, what you were suggesting earlier the impact of mission and then you could say one to 10 only give me everything that's a five, only giving me everything that has a, falls under 10 that might help with the feelings like politically correct. are you turned in liking the naming is not that important right now? Once you guys see the prototype, I guess, with that being visually in front of you and makes a little bit easier to see, oh, that value, it's important that value is not important,

Speaker so that kind of leads me to another question. And again, I don't know what they gave you for requirements as far as the findings. To me, I see it that the finding should be worked in two different phases if your using print. One is when you're on site....

Recording 6

Speaker One is when you're actually writing your report. So, let's say like, for instance, when you're on site and what I like to see is affected IP. So, what is the issue, how you exploited it? And what is your mitigation strategy for so essentially your recommendation How you going to fix I mean, I like to see that but once you get once once you're outside and you're here, your she'll be your analysis, because I mean, you don't have a lot of time to do analysis on site. So, once you're once you're outside, you're doing your analysis. I want to say I want to see I want information that's going to help me populate my risk matrix. So essentially, I think you touched on the risk matrix earlier to students. So, I want to know more information on the particular system. Is this critical system Yes or no? Blah, blah, blah, like different little things like that. That way when when they give my when a general my report, essentially have almost everything filled out, So I want to automate as much as possible. I don't want to take that much time. And

Speaker so. So, what you're seeing is, is you have the finding the right, and the artifacts and the right. And then like, down here, we're like, technical impact, score of based on that we already use. Right, right, six mitigating factors too, right?

speaker For instance, I mean, maybe they can be grayed out during the assessment. But once you get outside then if you time at the end

speaker We have, we have this algorithm, it’s kind of like some little algorithm. It's a little formula that you put certain values and then it gives you a grade at the end. And based on that grade, that's going to be you know, high, medium, high medium. medium low.

Elsa I think Vince put in, hinted at that. Yeah, and the RDD and we did that on purpose. So that during the interview you guys to talk a little bit more about or the students could start asking questions. That was one of things I wanted to put into the system because it seemed like it's doable within the context of what the information that we have just so we need the formulas and then we need the appropriate fields in order to generate the output the job. Okay, so get back, I guess at a later time for now, which just name it out brief. Yes or no. You see vulnerability. Yeah. I think for so for the, the report or you guys are going to provide a template. Okay. So that should answer a lot of the questions that we have under there. What else are we missing here.

speaker Will do awesome report templates.

Elsa Because what I was telling the students is that we really need to want so this class, they're learning how to ask questions. One of the things I dealt with them in the class, I say, hey, do you really know what a technical report is? Let's say in there, one of the value we need to privileges is a risk value, like you mentioned earlier, with the type of input, are we able to generate this output? If the answer is no, there are something that we're missing. That's the example that I gave them. So, if you guys could give us the technical report, and then we could start analyzing, hey, this is what you need to see here. Do we have all the necessary input in or generate that output one of the models they're going to do is called data flow diagram? So, they go to identify what are the processes, given this input, are they able to would output as a system expected to generate and is it matching with what you guys are asking for. So that's another type of analysis their gonna do.

speaker I'm thinking it would be nice if we could do like a little makeup system. And then do the ERB, the risk matrix that risk analysis and then sample report and just say, look,

speaker you know, in thinking about a report, I know Philip has his own little side thing that he's doing with on how to auto generate report when maybe there's something that we can talk to him to see if we can incorporate what he's trying to present because as far as I know, I mean, I don't know the whole story, but I think we we contracted some company, this has some software that auto generates reports for you. And we want to say contract with them that is that we've had them. We paid them in order to modify their their product for us. And maybe that's something that, that we should talk to him about as far as the final report.

Elsa Yeah, so that could be a potential system that we leverage on. So, our system, again I don't know what this other system does, if all it does is say, Hey, take all those data and then spit out a an output based on this specified template. Then our system doesn't so our students, when they do the development, they don't have the code that all we have to do. Make sure that collect Everything that you guys need, and then we send it out in whatever form and then they take it as an input to their system.

Speaker or also Maybe your product is actually better than what we're doing.

Elsa So, I'll wait for you guys. So just a couple of questions. We'll wrap up. So, data syncing, the students are going to do the analysis, data storage. I think you guys touched on it already about all having the data in the hard drive and then archive it. Let me see, are there any preferences on data basis?

speaker I guess What's the... No, no, I was gonna say because it's not Oracle.

Elsa Non-Oracle? Okay. Okay.

speaker Just because there's syntax's and I know there's a couple of guys that are pretty familiar with Oracle. But I mean, like the rest of us,

Elsa okay. So, there are no like, specific technical requirements as far as the type of database at the student should know more.

speaker What our image has to if we can leverage something that we already are using,

speaker I think we use my skill. No with the P, there's a p in there. Oh, Postgres, PostgreSQL

Elsa because the next phase is that the students are going to take all the needs, and then start breaking them down into components. So, one aspect of the system is for them to store data. So, they're going to start going out there to look at existing products. So, databases are different types of structured and unstructured and

speaker they're going to be like dashboards for us.

Elsa That's interface that's coming up. Since you brought it up interfaces, are there any specific requirements?

speaker The only one that I hadn't heard, and I think you touch on it, Yeah, we were looking at a web interface. Yeah.

Elsa If you could confirm that and and get back to me on security, any specific security requirements as far as like authentication, any communication protocol, any encryption required as a system store any sensitive data that?

speaker Yeah, I would say I mean, regards to that. I mean, we can use SSH to transfer data as opposed to saying, I don't want to send clear texts protocols their texts. No, no, no, no. No.

speaker No. Yeah. From more enough to be I guess, everything secure. SEP. Virtual copy. Yeah, no, no, no regular copy

Elsa Okay.

speaker So, there's also SFTP against if it works. As far as the login to the, to the to the database, how do we do uploads do we...

speaker We got to authenticate

speaker The system just authenticates we just hard code the authentication.

speaker I Don't think we've hard code well I don't remember if we hard code the database uses a web interface, force it to use HTTPS, as opposed to just HTTP. This is a web interface, Yeah, you know what screw the feature we should focus on that because I mean we are the security I've heard people say hey, you're preaching all this security stuff with them and you're doing certain things.

Elsa Because we have other systems that we work with develop for you guys. The security aspect because you guys have worked in likely the the environment you guys worked in, in the collaboration work. And the past we were told them that don't worry about that authentication. And don't worry about this and don't worry about that. That's why the students are asking for this particular project. Lastly, for development constraints, programming languages, any?

speaker I think Vince had an idea, but that right? He said something about he was gonna coordinate with you, not necessarily tell them but kind of like guide at some point them to

Elsa for languages I thought he said Python.

speaker Yeah, no, no I know. But I don't know if he wanted to tell them that, I don't know that's at least what he told me.

Elsa So okay, so I guess Python operating system early on we talked about compatibility both Linux and Windows, right. So, you're going to get back. So, for 57 the type of system that will be implemented web application system application but let me know. And the last question Will the system be used in the local area network or will it allow us to access communicate or transfer files through a wireless connection?

speaker Oh, that would be nice, that would be nice to have. Okay.

Elsa Nice. The wireless connections Yeah.

speaker Yeah but more than likely, most of the time it's going to be a local and Lan Thank you. Thank you everybody for being this morning. This was NPR

Unknown Speaker when

speaker our egos are being attacked ranging

speaker from let's say location location. This is

speaker one large enough

speaker this is a mystery What is it Dr. Frasier crane.

Elsa Hopefully the recording is got

$