Jesus’s Transcriptions.

Morning Session 0:00-16:00

Speaker 1 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 2 00:22

Chelsea Manning?

Speaker 1 00:23

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

Speaker 2 00:37

USBs?

Speaker 1 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.

Unknown Speaker 01:42

I know the I is integrity.

Speaker 1 01:44

Integrity, very good. See, just guess. Confidence.

Unknown Speaker 01:56

Confidentiality? Availability.

Speaker 1 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.

Unknown 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?

Unknown 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 1 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 2 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 2 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.

Stopped at 16:00

Our Session 0:00-14:00

Speaker 1 00:00

What happened?

Speaker Unknown 00:02

Their app failed.

Speaker 1 00:05

Their app failed. Why did it fail?

Speaker Unknown 00:08

They didn’t test it well. We don't know.

Speaker 1 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 2 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 Unknown 01:26

Writing a report on this.

Speaker Unknown 01:28

Going to the career fair.

Speaker 2 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 1 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 2 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 3 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 1 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 tha 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 2 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 1 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 2 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 1 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 2 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 1 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 1 13:36

Okay. So So we do have a current solution, or a semi workable solution, or we have some of the things that we like, I think we've, we've identified on the RV. 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 sends my information to yours and yours to mind. 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.

Stopped at 14:45

Afternoon Session 00:00-19:21

Speaker Elsa 00:00

Finding is already attached to a sub task or a task in the current system already no?

Speaker 1

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…

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.

v

So, yeah, I don't want to say, should we just captured as a

visor?

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 2

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 2

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 2

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 2

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 1

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 1

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 eachother.

Speaker 2

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 2

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 1

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 4

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 2

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 2

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 1

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 2

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 1

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 1

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 1

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 2

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 1

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 2

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