**CSD 101 - Day 5 - Escrow, Release Channels, Monitoring, Incidents, Track It Release**

0:04  
All right, welcome to day five, the last day for CSD 101 for us together.

0:11  
I will take this chance to say that while it is our last day for this series, I'm always available for questions and James's too, and so you can always reach out to us.

0:22  
I'm Namratha B James is James Weigart JAMZW.

0:27  
You can always reach out to us at any time if you just want to chat or if you have questions or if you are trying to find a contact.

0:35  
We may not know all the answers, but we definitely know who to go to for answers and we can help redirect you.

0:42  
I'm, I'm pleasantly surprised and always happy to hear from people who took CST 101 like months and months ago or a year ago and said, hey, I need some help, you know, finding a contactor, figuring out where to go.

0:55  
So I'm always happy to hear from you guys.

0:58  
All right, before we jump into the content for the last day, let me take a second to pause and ask.

1:05  
Are there any questions from what we covered yesterday?

1:09  
We talked about the non security workflow, we talked about some of the the packaging and some of the validation efforts.

1:17  
And so I just take a moment in case there are any questions before we move on to what is next.

1:27  
All good.

1:28  
All right.

1:29  
As always, please feel free to ask questions.

1:31  
You can put them in the chat window or even just speak up and we will pause.

1:35  
We're happy.

1:36  
This is completely meant to be interactive.

1:38  
So let's move on.

1:40  
We have done all of our fixes.

1:42  
We have built and packaged and done validation and done the appropriate turns that are required to address issues found during validation, and we're almost ready to ship.

1:51  
So we enter escrow and I briefly talked about this when we looked at the whole release timeline.

1:58  
So I, I will, I will try to be brief.

2:01  
Escrow is this concept where you kind of hold steady, everything is done, you have the final bits.

2:07  
That's the idea behind escrow.

2:09  
If you have worked in other teams at Microsoft, you might have heard this terminology as well, including in the feature teams where they say, hey, escrow before we ship the product, right, Everything's done, we're holding steady.

2:20  
And this is the time when you do really need an exception and a good justification to churn.

2:29  
So anytime after the check in deadline, you know on that timeline that we looked at, you need an exception to churn.

2:34  
But the bar goes really high during escrow week because you are just, you know, days from Patch Tuesday.

2:41  
Remember our principles about DE risking that release.

2:43  
So you that you know, you'd need to have a really good reason to need to churn during this time.

2:49  
And some examples of why you would churn during this time are on the slide a SERP.

2:54  
And of course, now remember that if a SERP is found during escrow week, you know, we are looking to assess it and then see if we can de escalate or mitigate in some way.

3:02  
And and then check if we can put it in the next train, right.

3:06  
If you know, if we're in escrow week, we're we're we're going to have to really make this decision of do we take this fix for the surf during this B that's coming up next week and how, you know, introduce some risk to it or do we put it in the following B?

3:20  
So that discussion will happen and you know, a lot of things will go into that.

3:24  
How close are we to the next B and how severe is the security issue and how how exploitable it is?

3:32  
Do we have any ways to kind of mitigate it, right.

3:34  
All those discussions will happen in ship room.

3:36  
Another example might be a crit set that we really can't wait for a following train or if during the two weeks of validation, MTP week one and week two, we found a high severity issue and we have to turn into escrow week to address it.

3:51  
So those are some of the times why you might be churning during escrow.

3:54  
The idea, however, is to hold steady and this is where teams are doing all the work so they can enable sign off on the Friday of escrow week.

4:02  
This includes, hey, have you triaged all your issues that were found during validation?

4:07  
You know, have you closed out all your bugs?

4:09  
Have you made sure and you know, looked at all the risks on the on the various reports that we have for the release, right dotting the IS crossing the TS And then on the Friday you're going to do have sign off.

4:20  
You're going to do sign off for all of our down level OSS, right?

4:24  
That's going to be CSD for the latest in market.

4:27  
It will be the feature team plus CSD, right?

4:30  
Sign off is, is a joint venture for the latest in market.

4:35  
And so all of our engineering managers will be the ones to do sign off from the CSD side.

4:41  
Any questions on escrow, the activities during escrow or discussions during escrow.

4:51  
And again, I'll encourage you all do not hesitate to jump into those ship rooms and listen in and see how that runs.

4:59  
I really would encourage you to to do that.

5:02  
I, I completely agree with James.

5:05  
If you have a local ship room, attend that and you're always welcome to attend Central ship room.

5:11  
The invite goes out to everybody.

5:13  
You're welcome to, you know, call into the team's call and just listen.

5:17  
And I will say again, ship rooms can always be a little bit intimidating if you haven't attended them before.

5:22  
Always seems really bizarre.

5:23  
People are talking really fast and kind of without context.

5:27  
It's by design and, and there's a certain rhythm to ship rooms based on the rhythms of the releases and it's always a continuing conversation.

5:37  
So please don't be discouraged.

5:39  
Attend shiproom.

5:40  
You may hear things that you don't understand perfectly fine after the shiproom, you know, ask your lead, ask your peers, maybe ask your shiproom driver.

5:50  
Hey, I heard you guys talking about this.

5:52  
What does it mean?

5:53  
Everyone is usually very, very open to questions and happy to help.

5:58  
So, you know, please take advantage of that.

6:01  
And then as you attend over time, you'll, you'll understand the rhythm and, and, and the context and the flow as well.

6:08  
And, and the link that I sent to you guys that has all three of the, of the ship rooms that CST has, there is just a meeting invite that you can click and add to your calendar.

6:17  
So it's, it's very open.

6:18  
It's on the SharePoint side.

6:20  
You can go and look at the notes from past.

6:23  
So that's all there.

6:24  
Absolutely.

6:26  
All right, So escrow has happened.

6:28  
We've got sign off and we're ready to ship.

6:31  
How do we send these fixes out to customers?

6:34  
Well, our SSD team, right, has the pipeline.

6:38  
They have the publishing pipeline where they publish to our customers.

6:41  
Where are they publishing to?

6:44  
We have some a variety of release channels.

6:48  
We have some channels that are the ones you're going to hear about the most.

6:51  
So we'll start with those.

6:52  
That's Wu, Windows Update W Sauce, Windows Server Update Service and Catalog.

6:58  
So let's let's dive into each of these in a little bit of detail.

7:02  
Wu is a channel that you'll often hear people talk about it as a consumer channel.

7:08  
It is, of course, available to any customer.

7:10  
You know, we don't restrict who can access who, but we definitely think of it as a consumer scenario.

7:15  
This would be the scenario of my mom.

7:17  
She's at home, she has her laptop, you know, and she's using it to just, you know, chat with the kids and look up, you know, look up things on the Internet.

7:26  
And her machine will be connecting to the Wu service directly and saying here's my attributes, what do you have for me?

7:32  
And it'll be sending down the updates and that her that she will consume.

7:36  
Definitely a consumer play.

7:38  
You typically don't have enterprises using Wu.

7:42  
You can think of Microsoft itself as an enterprise.

7:45  
Our Microsoft issued devices are not directly speaking to Wu, right?

7:49  
Our CSEO team, right, which is our IT organization, they are controlling what gets pushed to all of these devices.

7:56  
And I think I mentioned yesterday or day before, you know, when a security update goes out, they have a charter and a goal to get those security fixes out to 95% of the devices in two weeks.

8:07  
And they do it in phases, right?

8:08  
And so our devices are part of that, right?

8:10  
They're, they're, they're pushing updates out so enterprises typically do not point their devices to Wu.

8:17  
That's why you'll hear people talk about it as a consumer channel.

8:20  
Then you.

8:21  
So what do enterprises actually use?

8:22  
Because they must be using something so they use WSUS or catalog.

8:26  
So WSUS is really, you can think about it as when we publish updates to Wu, they also go to WSUS, right?

8:33  
And then enterprises usually will set up their own WSAS server or some other third party solution and that will contact the Microsoft WSAS server will sync all the updates down.

8:45  
They will then on their side be able to look at the updates and approve what they want to push out to their organization and how they want to push it out.

8:55  
So you can imagine that there's an IT admin they will look at on their server side what has been synced down from our WSAS server and they'll say, OK, here are all the security already fixes that are applicable to my organization.

9:08  
I'm going to approve them.

9:10  
Uh, and I'm going to roll them out in four phases.

9:14  
On the first phase might be maybe to some test machines on day one and if everything goes well, phase two might be, you know 10% of the devices in the organization and then they kind of monitor how that goes.

9:26  
And then phase three and phase four.

9:28  
So that's an example of how an enterprise might might do that using WSUS.

9:34  
I do want to call out a couple of things that are interesting about Wu and WSUS.

9:39  
Not only are the updates being pushed there, but they're being pushed with some metadata around them.

9:46  
And this is where you'll hear people talk about targeting or, or or publishing logic or offering logic.

9:52  
These are some words you might hear.

9:53  
So this isn't, and let me give you an example.

9:57  
When you have an OS version like RS3 and if the consumer skews have hit end of life and the and the commercial skews are not end of life.

10:07  
So home and prohibit end of life, but enterprise and education have not hit end of life.

10:13  
Then when we publish the updates to Wu and WSUS, we put logic around them that says, hey, only offer this to an RS3 enterprise device, don't offer this to RS3 home device, right?

10:24  
Because they're no longer in support.

10:26  
And because we build in that, you know, when that customer takes that update, right?

10:31  
If they try to take it, it actually won't install.

10:34  
It'll give them an error message, it'll say this isn't applicable to your device.

10:38  
And so why would you offer an update to a device that actually can't install it?

10:42  
That's a terrible user experience too.

10:44  
And so Wu and WSAS have this concept of offering logic where the, when the updates get pushed out, they have this metadata around them that says whom should they be offered to?

10:56  
And, and, and so when an IT admin is looking in WSAS and they're looking at all the updates that have been synced down from our WSAS server into their system, they can look, they, they, they, they, it comes down with this metadata, it comes down with this offering logic.

11:12  
And now let's talk about catalog.

11:15  
So catalog is also an enterprise channel.

11:18  
I kind of think of it as Amazon, but not quite with the same UI.

11:23  
You can actually go access catalogue.

11:25  
You know, there's a URL for it.

11:28  
James can put that in the chat window for you guys.

11:30  
And you can just go in and search for what you want.

11:32  
You can search for a certain KB number.

11:34  
It will pop right up.

11:36  
You can say add to my cart.

11:37  
It's totally free.

11:38  
We're not asking for any money because these updates are part of our promise, are part of our life cycle.

11:43  
And then you would download it and then you can go apply it to, you know, whichever devices you have.

11:49  
Why is this an enterprise channel?

11:50  
Because, you know, my mom uses Amazon.

11:52  
Why wouldn't she just go to catalogue?

11:54  
Well, first of all, you know it again, it doesn't have quite the same UI as Amazon.

11:58  
And so you really do have to know what you're looking for, right?

12:01  
You have to know what you're searching for.

12:04  
And then you kind of have to be able to navigate through all the details and then be able to download and then distribute, right, the updates to your devices.

12:12  
Some enterprises like to use catalogue because you know for a variety of reasons they may not have the ability to set up an infrastructure like their own WSS server or they might just feel like they have more control there.

12:25  
We also of course use catalogue for remember some of the out of band releases like our crit sets that go out of band.

12:32  
Now the interesting thing when we push an update to catalogue, it does not carry the same offering logic that same metadata with it.

12:40  
So if you have an RS3 update that's going out, that's for enterprise only and not for home.

12:47  
You know, if you scan against Wu or WSUS, it will evaluate correctly.

12:50  
Oh, this is an RS3 home device, Don't even offer it.

12:53  
Don't even show it.

12:54  
Whereas do offer it and show it to an RS3 enterprise device and catalog.

12:58  
There is no such concept.

12:59  
You can go search for whatever you want, download whatever you want.

13:02  
This is where then our packaging level applicability kicks in.

13:06  
And when you take that update and try to put it on an RS3 home device, you'll then get that error message.

13:11  
But this is where you know none of that offering logic comes along.

13:14  
And so it is a little bit more of a power user scenario, right?

13:18  
You have to know what you're looking for.

13:20  
You have to understand that you don't have any of this offering logic around there to kind of help make intelligent choices or decisions for you and you can go get what you want and then may or may not work on your device, may or may not be applicable.

13:33  
So I'll pause for a second before I get into other channels to ask if there are any questions or James would you like to add anything?

13:40  
Yeah, well there is a question that we are, there was a question about inclusion and exclusion list.

13:47  
And your second point, Miyabeka, is, is the offering logic include the inclusion and exclusion list which determines which servers and systems are applicable.

13:58  
And yes, and Namratha will probably go into more detail on this, but we also have two different systems that we're operating with to do this.

14:09  
We have an older legacy system and then we have this newer system.

14:12  
And so the, the concepts are basically saying, but how they do it is a little different, but correct.

14:17  
Yes, that is, that is how we say, hey, if you are a server with this type of processor, don't install this like we do kind of have that that those levers of applicability we sometimes call it or offering logic and we can't say include this or exclude this.

14:35  
Another lever that we have is sometimes we can say only go to this region.

14:42  
For example, we could say only go to the EU, only go to the US and that sometimes helps us mitigate problems or solve certain solutions.

14:53  
So what's kind of important for CFE folks and, and, and yes, and SSD is when there is a problem, what are all the knobs we have that can be used?

15:06  
And, and you'll find in shiproom, you'll hear this discussion a lot, which is, hey, well, what if we did this, if we turn this up and we did this because we're trying to evaluate a way to mitigate a lot of times and, and, or, or reduce the impact of an issue that has happened, but at the same time, not disrupt people unnecessarily and also not cause more risk where all these things are in a way.

15:29  
That was a great segue.

15:30  
Let me talk a little bit about some of these levers.

15:33  
And let me also talk about when we use these three channels, because I said these are the most common, no Wu and WSS and catalog.

15:39  
So when we have security fixes and they, they, you know, they go out on the B week, right?

15:43  
Of course, they go to all of these channels, Wu, WSS, catalog and they go out to everybody at the same time, right?

15:52  
There is no concept of, you know, sending it to some regions and not other regions or sending it to some percentage of users and not other users or some configuration of, you know, devices.

16:04  
No, goes to everybody on patch Tuesday at 10:00 our our Redmond time to Wu SUS and catalog.

16:12  
Now the, the, the list that we're following here is what is it's applicable to, right?

16:18  
We're sending it out to the OSS and the devices that are applicable or in support, right?

16:24  
When we have non security fixes going out, they actually don't go to all these channels.

16:29  
They go to W SUS and catalogue.

16:31  
Because the idea here is that this is again, more for enterprises, right?

16:35  
For a consumer like my mom, she just gets updates once a month right from Wu unless she goes and seeks them somewhere.

16:44  
And so they, they, you know, we push it out to SUS and catalogue, right?

16:48  
And, and, and those enterprise admins can go and look for them and deploy them.

16:56  
And there's some additional levers.

16:58  
James talked about regions.

17:00  
This is where we call it geofencing, and this is where you can say offer to this country only or offered to the set of countries.

17:08  
We use this in a couple of different ways.

17:11  
I'll give 2 examples.

17:13  
One example is exactly what James mentioned, which is that we have a problem and we need to mitigate it, and we want to restrict it from not going to a certain region.

17:21  
We had an example of this where we had a fix that went out and for because of the kind of fix that it was, it broke OEMs in China.

17:32  
And So what we did was we stopped offering it, offering that, offering those updates to China, but we were offering to the rest of the world.

17:38  
So geofencing was used for that.

17:41  
Another, another way.

17:42  
And another reason we use geofencing is when we do feature rollouts, when we have a new version of the OS right going out the door.

17:49  
And I mentioned I think maybe on day two that when we push those out, we don't just push out a new version to the whole world on the first day at the same time, right?

17:59  
We don't say, hey, 2004 is here, everyone go get it right.

18:02  
We actually have a really complex matrix that we go through.

18:06  
There's a lot of analysis and a lot of data mining done and a lot of thought put into it.

18:12  
And they start with, you know, OK, a small region in a small one country and devices that you know have space that have you no good network, etcetera, etcetera.

18:24  
They come up with this whole matrix and they first start there and then they monitor and they look for issues and then they expand.

18:29  
So it kind of goes wider and wider and wider and wider over the course of several weeks and sometimes several months.

18:35  
That's another time when we would use geofencing where we'd say hey, first time we're only going to send to Canada or Australia, right.

18:41  
So that's another example or is geofencing.

18:43  
We also have the ability to throttle.

18:45  
This means that instead of offering the update to 100% of customers, we can either throttle and offer to zero.

18:51  
That's one option or we can even throttle and say we're offering to 60% of customers or 50%.

18:56  
So this these are different ways as well that we can do that different levers that we have.

19:01  
There are also additional levers that we have where we can say, hey, offer it to all customers except do this certain chipset or except to devices that are of a certain make and model or devices that have a certain registry key.

19:15  
We don't do that all the time.

19:17  
It doesn't happen all the time, but every so often we run into a problem where we're like, oh, we broke certain functionality on Surface Hub devices.

19:24  
We need to stop offering, you know, to surface up and so we'll say, OK, don't offer to that edition or we'll say, oh, we broke, you know, certain Lenovo devices and so don't offer to that.

19:34  
So we have those levers as well.

19:35  
These are examples of levers.

19:39  
Any questions or James, did you want to add anything to that before we go to other channels?

19:44  
Well, there was there was a couple questions that was really interesting from from Yasser around, Hey, you know, for WSUS is, is using the old update mechanism.

19:53  
Does that cause problems?

19:56  
And you know my reply was WSUS is a pretty tried and true technology.

20:01  
In fact, we haven't been updating WSUS for many, many, many years.

20:06  
It is a very old technology, but it is used extensively in enterprises.

20:12  
And kind of to give you a better answer, Yasser, We have problems through the whole pipeline at times.

20:21  
There's not one area where I can say we don't have a problem that gets discovered here and there.

20:27  
We do have areas of problems like it's often that we will have install problems.

20:34  
We don't know why we have to go figure them out.

20:36  
We can have pipeline problems.

20:40  
And so how we track all of those is through incidents.

20:43  
So whenever something doesn't happen correctly, we we log an incident and then we go and try and solve it and fix it.

20:50  
And then of course to try and make as we never have it again.

20:53  
But I can't say that there's really one area over another that we find problems or not on.

21:00  
They're they're they're kind of through the whole pipeline and we all work to solve them.

21:04  
That's why understanding all of this is important no matter what team you're on, whether you're CFE, SSD test base or because you will be encountering all of these and something doesn't work and we have to figure out why.

21:18  
That's right.

21:19  
Did we answer your question, Yasar?

21:25  
Because if not because I'm not because you talked about.

21:27  
Yeah, OK, perfect.

21:28  
You talked about missing updates.

21:28  
I wasn't sure.

21:29  
And then James alluded a little bit to the old system and the new system.

21:32  
And so just again, because we would like for you to walk out of these five days with some good terminology, you know, in your mind.

21:38  
So when people are talking to you, you're aware there's actually the back end old systems and then the front end old systems.

21:45  
So on our side there was the publishing pipeline that was called S e.g.

21:49  
Dr.

21:50  
which is mostly deprecated now.

21:52  
Woop woop.

21:53  
And the new system is called One Pub.

21:55  
And the idea was to go from this very manual system, which also, you know, had a ton of levers and configurability.

22:03  
So that was great.

22:04  
But it was all very, very, very manual to moving to a much more automated and templatized system.

22:09  
And that's the one PEP system.

22:11  
And you'll often see status reports from their team and I'll have little robots.

22:17  
And that was the whole idea was to like automate, right?

22:19  
Templatize and automate.

22:20  
It's we have the little robots and it's been fantastic.

22:23  
It has reduced a lot of the incidents that we have, a lot of the errors that we have, right.

22:28  
You can imagine when you're manually trying to, you know, get all the right metadata, get all the right titles, get all the right applicabilities, you can make mistakes.

22:36  
So it's been great to have that.

22:37  
That's on our side, our publishing system, S e.g.

22:40  
Dr.

22:40  
and one pub for the most part, it should be unless you work in SSD and you work in the publishing team, it should be a black box to you.

22:48  
But it is good to know that we have these systems because every so every so often you'll be in some weird situation where you'll need to use one of the old systems, right?

22:56  
So good to know.

22:58  
Then there's our partner team, right?

23:00  
The the Windows Update partner team.

23:01  
They have an old and new system.

23:03  
They have the movie 6 system, right, Microsoft update version 6 system.

23:07  
And then they have the D CAT system, the new one.

23:10  
And so I think RS3 and above uses D CAT, below that is movie 6.

23:15  
There's also some nuances around the update types, right?

23:19  
If you work in the SSD space and publishing, you will definitely be getting very, very familiar with that.

23:24  
For the rest of us, when we encounter the need, you know, to maybe change these levers, right?

23:31  
And we have this conversation, that's when it comes into play.

23:33  
And so that's why you'll find that our friends from the SSD publishing team come to our central ship rooms every day so that we can they can be there for those conversations and they know and what levers are available on the old movie 6 system and what's available on the D Cat system and kind of the finesse that we have to change, change some of our options.

23:53  
All right, let's talk about some other channels.

23:55  
We do have some other channels.

23:56  
We don't talk about them a whole lot just because hopefully you're not using them a whole lot, but it's good to know about them.

24:03  
DLC stands for download center.

24:05  
It's actually a website.

24:06  
You can go to it, you could search for it, it would it would show up.

24:09  
It's it it, You know, we tried 345 years ago to deprecate DLC actually, didn't we, James Yeah.

24:18  
This was an old release channel and the idea was that whatever we put out, it would get put out on the DLC.

24:24  
We really wanted to deprecate it in favour of catalogue, right And Wu and WSUS.

24:29  
What turned out was there was some update types that catalogue, for example, could not support and therefore we could not completely get rid of rid of DLC because we needed someplace for those update types to land.

24:42  
So it's still around though you will find that, you know, for example, in our team, 99.99% of our content doesn't get published to DLC anymore, right?

24:52  
We've, we've published to the three channels, Wu, SAS and Catalog rarely.

24:57  
Once in a few years there'll be some small piece of content that you need to publish for some issue, for probably for some older technology that we still support and service, right?

25:05  
Not for new things.

25:07  
And we need to put the update out on DLC.

25:09  
An example of that Namratha would be the MDOP enterprise tools, which is, that's right.

25:15  
Those, those still update yeah, to to DLC because they're a very old technology.

25:22  
They're old are MSI.

25:24  
And MSI is one of the file types that cannot go on catalog, right.

25:29  
And interestingly enough, nobody is doing updates to catalog in terms of features or work.

25:35  
And so things kind of are that's why we still have to mm hmm 'cause we need someplace, right?

25:40  
You can't just have no place 'cause when we do have a problem and MDOP and we need to fix it, we need some place to land that update.

25:47  
That's an official channel yeah And and one of the problems with with uh, the DLC and umm Namroth is getting pulled into this heavily is that it is like 20 years worth of uh update code that is just sitting there.

26:03  
Nobody knows what it is anymore.

26:05  
And so there's not really a good clean up method on DLC and these other which is turning up and tackling that next guy.

26:16  
So the other, the other thing to, to think about in all of this, which is in everything you do, there comes a cost of maintenance and how and what is that cost and how do you think about it?

26:27  
Whenever we ship a Windows 10 version, one of our big lessons learned is wow, this new 6 every six months release, this is expensive to maintain.

26:38  
So there's a lot of of, of act and react, which is, you know, think about what we do and, and then think about the maintenance.

26:46  
Like we can't just kick stuff out and customers use it and then a problem happens, somebody has to go back and find it and maintain it.

26:52  
Yep, absolutely.

26:54  
This is a true story.

26:56  
All right, let's talk about SIH and Woofbee.

26:59  
So SIH stands for you know, man, every time, every time I do the series, I think Dang, what does it stand for?

27:05  
Self initiated healing, server initiated healing.

27:09  
OK, this time I'm going to find out and come back because every time I think Dang, I don't remember what the S is.

27:15  
Is it self or server?

27:16  
But it's actually self.

27:19  
Is it self?

27:19  
Oh yeah.

27:20  
Every time I forget it's self initiated healing for the Wu client, for the Wu client.

27:25  
So this is really, I think of it as a backdoor and it, it, let me tell what it is.

27:32  
It makes more sense why it's a backdoor typically, right?

27:34  
You have a Windows Update client in your device.

27:36  
It communicates to the service and it sends up some attributes about itself and it gets back information about what updates are available to it.

27:42  
So there's this contract that's happening, right?

27:44  
And this communication, every so often, not very often, quite rarely actually, we've run into a situation where somehow we have lost the ability to communicate with the device.

27:56  
Something has gone wrong on the Windows Update client or something has gone wrong in that communication channel, and we cannot actually reach this device.

28:04  
If you cannot communicate to a device, you certainly cannot update it.

28:08  
And if you cannot update it, that device is certainly not secure anymore.

28:11  
Now, when you're in that position, we can use the SIH.

28:15  
This is a back door because you are able to directly go and target that machine and send an update to it.

28:21  
But it's not through this established protocol, this established way of communicating.

28:26  
And so we are very careful about using SIH.

28:29  
It does require approval from our leadership, right?

28:32  
It's a little bit like walking into someone's house unannounced, right?

28:35  
You suddenly show up on their device.

28:36  
And we, we take that very carefully and very seriously.

28:39  
We want to be very respectful of our customers.

28:41  
And so we really think about is there any other way for us to contact these devices?

28:45  
Is there any other way for us to repair what's gone, what's gone wrong so that we can communicate with that device?

28:53  
And So what we do is we, you know, we, we really can exhaust all our other options before we before we use SIH.

29:02  
And I think typically when we have used it in the past, it's been from the CPC team.

29:08  
This was the the currency, right, And the cross-platform team and this is where we have devices that are usually sediment, right?

29:16  
They're out of support and they're not moving forward.

29:19  
And they've run into some weird situation that's kind of the, the devices backed into a corner, not able to get updates, not able to move forward.

29:26  
And we've used SIH to get get to those devices.

29:29  
And I think Ricardo has corrected us.

29:31  
It's service initiated.

29:32  
Perfect, thank you.

29:34  
I'm going to try and remember that.

29:35  
I always forgot.

29:37  
Then there's Woof Beat, and I'll be really brief about Woof Beat stands for Windows Update for Business.

29:41  
And this is basically this idea that we say, hey, commercial customers, you know, because not for all customers do they have a huge IT administrative staff and team and knowledge workers who can do that.

29:56  
You know, they're trying to run their business, they're trying to do whatever it is that they're trying to do.

29:59  
And and this is just part of I need my machines to keep working and being secure.

30:04  
So we say, OK, we can manage your devices for you.

30:06  
So you become a Woofbee customer and we manage like deploying updates to your device and moving your devices forward to the next versions so that you are always in support and not running an out of support version of an OS.

30:18  
So that's what Windows Update for Business stands for.

30:23  
Any questions I can answer on that or James, anything you would like to add here?

30:29  
Nope, nothing more from my side.

30:31  
The the reason that all of this is important to understand is because you will come to a certain point where you're like, I need to get something to my customers and you will have to make a decision what is the right channel?

30:44  
And so understanding these and knowing what they are and how they work is going to be important, correct.

30:52  
And I'm sorry about that Excel sheet that just splashed across I accidentally moused over in my taskbar Excel and that happened.

30:59  
Sorry about that.

31:00  
Oh and Ricardo corrected us both.

31:02  
It is service initiated, right?

31:04  
That's what I said Ricardo found IT service.

31:07  
Thank you, Ricardo.

31:08  
Remember that?

31:08  
I every time I think, Dang, I forgot what it was again.

31:12  
Yeah.

31:12  
See the power of acronyms, Ricardo, as the power of the wiki is the and is it?

31:18  
If I don't know it, I get to make it up.

31:21  
No, no, no, no, no, no.

31:31  
That's what it is.

31:32  
It's Friday.

31:32  
All right.

31:34  
Any questions?

31:35  
If not, let's move forward.

31:39  
Typically, I would love to give you a walkthrough, walkthrough of our tools.

31:42  
I'm not sure we're going to have enough time.

31:43  
So I'm going to skip past this.

31:45  
We do have a great recording from day of learning and I want to talk a little bit about what happens after a release.

31:51  
If we find that we have some time leftover, I will bounce back to that and at least bring up the track it release report.

31:57  
So what happens after release?

31:59  
You know, we've we've got the release channels.

32:01  
It's all been published, right?

32:02  
Everything is great.

32:03  
Well, so we do a couple of things.

32:06  
One is we monitor, right?

32:09  
We want to monitor that did the did the updates that we send out actually go live yes or no?

32:15  
That's that's what the first item there is live site verification test.

32:19  
And you know, in the past it used to be a manual test.

32:23  
Now it's automated.

32:24  
It's fantastic.

32:24  
We know whether updates actually went live and one, whether they went live, 2, whether they went live within their SLA.

32:33  
And it's very important to us because especially for security payloads, it's critical that when we publish them, it happened successfully and it's available to customers.

32:42  
And so if there's ever any problem with that, we really want to know immediately so we can fix it because we want our security payload to be available to all customers at the same time as soon as possible, right?

32:53  
So that's live site verification test.

32:55  
We also have the WAS lab that does monitoring after release.

32:58  
That stands for the Windows as a service lab.

33:00  
And this is really looking for the next step after LSVT.

33:04  
You know, LSVT says it's available, Wazzlab says, what's my experience with installing that update?

33:09  
You know, was it really slow?

33:11  
Did it require more than one reboot?

33:13  
It should have just been one reboot.

33:14  
You know, things like that.

33:16  
It's looking for those experiences.

33:18  
And it's also monitoring for trends over time.

33:21  
You can imagine if the experience deteriorates just a little bit every few months, you may not notice month to month, but if you look at it over the course of a year or two years, you're like, wow, it really deteriorated.

33:30  
So Wazzlab is really great for that.

33:32  
We monitor, we monitor the woof funnel.

33:35  
This is the Windows Update funnel.

33:36  
This oh, I should take a step back and map this to teams.

33:39  
LSVT and WAZ lab is done by the SSD RAM team.

33:44  
So Christaberski and Jim Cauzi's org, the Wu funnel.

33:47  
This happens in the CPC team, Cornell and Key and Gabe's org.

33:52  
They are looking for what's going on with the Windows updates that we're offering.

33:56  
So the, the reason they call it a funnel is it starts right at the top.

33:59  
You know, these are all the devices that are eligible to take updates.

34:02  
These are all the devices that scanned, these are all the ones that we offered to, these are all the ones that started the download.

34:07  
These are all the ones that successfully, you know, actually downloaded.

34:10  
These are all the ones that successfully opened the package and installed it, right?

34:14  
And it gets narrow and narrow because of every point, right?

34:16  
You have either errors that happen, which is the corollary to the Wu funnel as they look at the errors, or you might have devices that, you know, they lost network or they dropped off or somebody just, you know, didn't notice something was happening in the background and just shut down their machine, right?

34:30  
Maybe close the laptop.

34:31  
So there's the woof funnel.

34:32  
We're monitoring that.

34:33  
And what we're really looking for, again, is these huge anomalies, right?

34:37  
If typically the funnel looks something like this and suddenly, you know, we're looking at a woop, the funnel suddenly narrowed very quickly at a stage where we didn't expect it to.

34:46  
What happened, right?

34:47  
Is the file corrupt on some of the servers?

34:51  
Is there a problem with our package?

34:53  
Right?

34:53  
So we're looking for anomalies, adoption.

34:56  
Adoption tells you how many devices have taken an update and we're of course, we want everyone to take the update on day one, hour 1, but that of course doesn't happen.

35:06  
And so we have this model of what we expect adoption to look like and then we're looking for anomalies to that model.

35:12  
This will find when there's a large variances and a great example of this is a few years ago when we published the update, you know, to our, our Windows Update partners.

35:23  
And then they basically, you know, because we have all over the world, we have customers.

35:29  
They then replicate that out to their servers, right to their data centers and to their CDNS.

35:37  
And so one of the CDNS actually there's two great examples.

35:41  
One of the CDNS one time had got content from us and content from another org at the same time and they were seeing a lot of customers connecting and downloading, right.

35:52  
They were going way over the bandwidth that they were expecting.

35:55  
They throttled our security updates.

35:58  
This is a no, no, don't throttle security updates.

36:00  
Everyone needs to get them.

36:01  
We found that out because adoption suddenly dropped.

36:05  
And then another story that I have about that is many years ago, we again, they were replicating out to the different CDNS and in one of the nodes, I think it was in Singapore, it got corrupted.

36:18  
The file got corrupted.

36:19  
No one noticed when it got copied over that the file got corrupted.

36:22  
And so customers were trying to download and of course, it was all failing because the file was not valid anymore.

36:29  
And we suddenly saw this huge drop in adoption because there's this whole region where customers are not able to install an update.

36:35  
We're like, what's going on?

36:36  
We found out about that and we were able to address it.

36:39  
So adoption will show you when there's a large, when there's a large drop, something big has happened.

36:45  
And we'll also pause from one second from the monitoring to say, because I didn't talk about this when we talked about the principles of the B release.

36:52  
I know I talked about de risking, but this example of the adoption and of the, the CDN throttling the security update reminded me it is so important for us to de risk the B release that every month, a week or two before the B release, because remember it's security releases for Windows sequel Office, right across the company.

37:14  
We actually review the payload company wide for Patch Tuesday.

37:20  
And so Carlos, who's RCVP and Mike Fortin, who's his manager, they come in and they sit down and teams come in and they say, here's the payload that we're releasing and they walk through it.

37:30  
And if there's anything that's not security, it gets booted out of C out of the out of that release.

37:34  
It gets booted out of B week and they are told to come into C week, right?

37:38  
Because it's not security.

37:40  
They don't want to do anything during patch Tuesday to risk that release.

37:45  
They want to have highest quality and they want to have least noise.

37:49  
So if you ship something that's non security and then something goes wrong and it generates all this press and this noise, people don't say, oh, that one non security fix went wrong.

37:58  
They go, oh, patch Tuesday.

38:00  
What a pain.

38:01  
Don't want that.

38:02  
And they want customers to have confidence that if I take what's what's shipped out on patch Tuesday, it's high quality, it's going to work and yes, I should keep taking it every month so I can be secure.

38:11  
And so they literally actually review the content company wide that's going out on patch Tuesday.

38:17  
So I just want to share that really quickly.

38:19  
I'll talk about social and CSS and then pause for questions.

38:22  
Again, other monitoring that we do, this is also done by socialist, done by the SSD RAM team.

38:29  
They are monitoring all the different social sources.

38:31  
Twitter is a great example.

38:32  
A lot of influencers are posting there, but lots of, you know, just regular people too.

38:36  
Technet where you have more of the IT admins, patch management, which is actually an e-mail list.

38:41  
It's an awesome source because it's, again, IT admins.

38:44  
And so the content that you get is really high quality, right?

38:47  
There's not, you know, it's not like Twitter where someone's talking about the hamburger I ate and you know, they're talking about Microsoft in general.

38:52  
And then, oh, here's an issue with my update.

38:55  
Patch management is usually all about, hey, I'm running an issue with my patch.

38:58  
And in fact, they will often troubleshoot and do a few levels of investigation.

39:02  
Really high quality source and they keep expanding the different social places that they look at, social avenues they look at.

39:09  
And what they're really looking for is are we, are we seeing anything anomalous?

39:14  
Right?

39:14  
There's always a certain amount of chatter, but are people suddenly talking a lot about an issue in one area or they're looking at, oh, you know, maybe there's just a couple of people talking about this on Twitter, but they're also talking about this issue on patch management or Technet.

39:26  
They're correlating across sources.

39:29  
And then CSS, this is our customer support organization and they of course are monitoring.

39:34  
They're getting calls from customers and they do a triage and they bubble up the top issues to us.

39:39  
So that was a lot about monitoring.

39:41  
I will pause for a second.

39:42  
Are there any questions?

39:44  
And Namratha, just so you know, I've been showing them how track it like walks through all of these and tracks all of the different absolutely things we've talked.

39:52  
Yeah, about.

39:53  
So all of this really is tracked in one place.

39:56  
The RAM team does an amazing job of the tool set they've created for us to monitor this whole thing through inception, through release, and then post release.

40:06  
So absolutely, if you want to see how that's all tracked, because it's a lot of stuff, it's track it, right?

40:11  
And we'll try to do a quick overview of it.

40:16  
So if there's no questions, I'll talk about incident management really quickly.

40:19  
I won't actually go into all the bullet points.

40:21  
It's a lot.

40:22  
We actually have some really great Brownbacks from the incident management team, from the serve team under CFE and we'll share some links out and and James, would you put some links to the Brownbacks?

40:32  
It'd be great.

40:33  
People, please go watch them.

40:34  
Very important.

40:35  
But let me talk a little bit about water incidents.

40:38  
So we've shipped something out.

40:39  
We are monitoring.

40:40  
We of course hope that nothing will go wrong, but every so often things do go wrong.

40:44  
We ship out a fix and something unexpected happens.

40:47  
Our goal, of course, is to catch it earlier.

40:49  
That's the validation.

40:50  
But sometimes we don't.

40:51  
So then we have an incident management process where we said, hey, we really need a way to, to, to have to take intake right, to get information about things that went wrong, to track them and to be able to act on them successfully.

41:08  
And so when anytime anything goes wrong unexpected for a customer, it's an incident.

41:14  
You'll also hear it referred to as a post release incident.

41:18  
And I'll talk about why it's called a post release incident because it's happened after we've released and shipped to a customer and there is another type of incident.

41:27  
I'll talk about it in just a minute.

41:29  
And so we log it in a tool called ICM.

41:31  
It's a Microsoft wide tool.

41:33  
Everyone has access to it and you and lots of teams use it.

41:37  
Teams that aren't using it are trying to conform their processes to use it.

41:40  
The idea is that everyone uses the same tool so that if there's an incident on that we find, but it's really related to Office or to Azure, anyone else, we can hand it back and forth to each other in the same tool with the same understanding.

41:53  
Every incident comes in and gets triaged, has severity based on the severity, you know, we have Slas for how quickly we need to react to them.

42:04  
And the other big thing I'll call out, other two big things I'll call out is that there is a call tree if, if there's an SLA, for example, that we need to acknowledge an incident in a certain time or we need to mitigate or resolve an incident a certain time, right, We have to meet those.

42:21  
But it, but if it's for example, very high severity of 0, there's a call tree where we say, hey, someone gets called and if you don't pick up, your backup gets called, right.

42:30  
And if that person doesn't pick up and it tries again, it goes up and up and up.

42:34  
That's why it's called a call tree.

42:35  
So for example, if I'm, if I'm on call for ENS and I don't pick up and my backup doesn't pick up and it tries us both a couple of times, it's going to, it's going to go up the ENS tree to our managers, then it's going to go up and up and up.

42:48  
And you can set up the call tree any way you want.

42:50  
We've set it up a certain way in CSD.

42:54  
And lastly, our goal is always to mitigate an incident as quickly as possible, stop the bleeding, stop the pain.

43:03  
And then of course, if there's a way for us to fix it, sometimes you'll find medication and resolution, maybe one in the same thing.

43:10  
And lastly, we are always looking to learn.

43:13  
And so that's why we do post mortems, right?

43:15  
So we can learn.

43:16  
And we are not just looking to tactically fix just that one issue.

43:19  
But is there a trend?

43:20  
Is there something bigger here that we need to learn and we need to take care of so we don't have such types of issues?

43:27  
Again, there are great brown bags from the from the surf team.

43:33  
A brown bag is basically it's a, you know, the idea was that it would be over lunch and you bring your lunch in a brown bag and you eat it and people will talk about something that you can learn about.

43:44  
But of course they don't always happen at lunchtime.

43:46  
And we have some great brown bags recorded by the surf team.

43:50  
And it would be, I, I think it'd be fantastic for you guys to go watch them, specially because you might be called upon in your teams to be primaries or backups for your area.

44:01  
I'll take 30 seconds to really say why did I say post release incidents?

44:05  
Does that mean there are other types of incidents?

44:07  
Ah, yes, there are.

44:09  
So especially folks in SSD and CPC will be very, very familiar with this, or at least you will become very familiar soon.

44:17  
All of our pipeline, all of our infrastructure, right, gets monitored.

44:22  
I I, I will refer you once more to the idea of building a world class service.

44:26  
There was a time when we actually didn't monitor much at all.

44:29  
And if things fell over, it was just, you know, somebody would notice.

44:32  
Oh, I was expecting a build or I was expecting a package.

44:35  
What happened?

44:35  
It didn't come out.

44:36  
Oh, let me go find out.

44:37  
Oh, something fell over, something failed.

44:39  
Well, this is a terrible way to, you know, for us to find out and, and then there might be a delay of many hours or even days and we have no good tracking and no good trends.

44:51  
How do we address problem areas, right?

44:53  
So SSD and CPC really took a strong hard look at this, started defining, you know, what should we be monitoring?

45:01  
And then once it started monitoring, OK, what are the areas we should be fixing, right?

45:05  
And they really made some incredible investments over the last few years.

45:09  
We could talk about that alone for more than an hour.

45:12  
So I won't go into a ton of detail about it, but just to say that they also monitor, right, their entire pipeline and when things go wrong, they file incidents.

45:20  
But those are internal and we kind of think of them as infrastructure incidents.

45:25  
And so I just want to to call that out.

45:28  
I'll pause for a second if there's questions about incidents and if not, then I will try to show the track of tool.

45:36  
Oh, I think I see a question.

45:38  
Carolina says I have a question about security fixes.

45:42  
Some fixes require reboots and some don't.

45:44  
The ones that do that's why we have patch Tuesday.

45:49  
Do the security fixes that do not require reboots get released by themselves optional No, all security fixes must go out on patch Tuesday.

45:56  
They absolutely must go out second Tuesday 10:00 That's right.

46:00  
And in fact, I think Carolina like the interesting is what what happens is if you have a non MSRC security and it needs a reboot and you need to get it out.

46:13  
The question is do you put that in the B?

46:16  
So it's kind of the flip flip you're thinking, which is all MSRC security must go out on that Tuesday.

46:24  
And if you have a non SEC that requires a reboot and it's important to go out, we have had these it it, it will happen, then you need to come and ask permission in the central ship room today.

46:37  
Can I put this non SEC in the SEC payload for these business reasons for duh, duh, duh, duh, duh.

46:43  
And it needs a reboot.

46:44  
If it doesn't, you would put it in the C and then in the following B you would get the needed reboot.

46:52  
So, so you just need to to time when the reboots happen if needed.

46:57  
Mm hmm.

46:58  
That's right.

46:59  
And then I think you also asked, are there security fixes that don't require reboots?

47:03  
And do we track which ones do and which ones don't?

47:06  
And I actually don't know the answer to that, James, are you aware of that?

47:10  
Yeah, the the answer is for security.

47:13  
If they are MSRC, we typically don't track whether it needs a reboot or not unless we are asked and then we will go find out.

47:22  
I will tell you that for the most part if you were in kind of ENS and below which is the different layers of the operating system, almost all of your fixes require reboots because most of those files are in use during normal running of the computer.

47:41  
And and the reason why C or non SEC don't require reboots usually is because they actually will sit there and it doesn't matter if they apply until the user just does a random reboot.

47:54  
But because we're trying to secure, we will force a reboot.

47:58  
So a lot of your non SEC could require a reboot, but it doesn't matter when it happens, Right?

48:04  
That's true.

48:05  
Any other questions that answer your questions, Carolina?

48:11  
Those are really good questions, by the way.

48:13  
Yep.

48:13  
And we love the questions.

48:20  
All right, I'm going to try man.

48:23  
It's, it's a lot to get through in 5 minutes.

48:25  
We're not going to get through it all.

48:26  
So we'll, we'll put in a link for Ted's brown bag on the, the track it tools.

48:32  
But I'm going to try to give you a really fast overview, AKA dot Ms.

48:36  
slash track it that, you know, remember that it's a very useful short link to get you here.

48:43  
I will call out that up here when you click on this app Switcher menu, you can get to all of the other reports as well that they have.

48:50  
This is the PLC that we've talked about.

48:52  
Here's some deep dive into social monitoring, For example, test reports for validation, right?

48:57  
So there's a whole slew of reports, and these are critical for our ability to run our business, to look at the trains to see what's happening over here.

49:07  
On the left side in the filters, you'll see that this allows you to see all the different products that we ship.

49:13  
They are kind of put into little buckets, right, to make it a little easier to find what you're looking for.

49:18  
Current branch, right?

49:19  
This is the the the one that's the latest in market 2004.

49:24  
And if you come down here, this says Windows 10 down level, right?

49:28  
These are all the other Windows 10 items.

49:31  
And then you'll see the 8.1 and earlier, right, what we used to originally call down level right there down here.

49:38  
And you'll see some flighting, which we talked about earlier for the active branch, right?

49:43  
That's why you see 20H2 and then others because yes, we do have a few other things that we ship as well.

49:49  
Anaheim SIH, we talked to your trusted root.

49:52  
So you'll see that there are lots and lots and lots of options here.

49:56  
And then here, these are all the different update types that we have, right?

49:59  
We've talked about some of these.

50:00  
We talked about LCUS, we talked about rollups, We talked about some speciality packages like SSUS.

50:05  
But we do have a few other update types as you can see, including media.

50:10  
And then these are the different releases.

50:12  
And so I have right now chosen all products, all update types for 5B for 2020.

50:16  
So that was May patch Tuesday.

50:19  
And you'll see on the side here, it's showing me a, a grid and it's showing me all the different updates here.

50:26  
And so I'm going to call out a couple of things in the first column here, you're going to see that it's going to tell you what the release was 5B because you can always select, you know, 5B and 6B or you know, things like that.

50:39  
So it tells you what release it was 5B and it's going to tell you what what OS it is, whether it's the insider program, that's what the active branch or for example, 2004, right?

50:49  
Then it's going to tell you in the second line what kind of update it is safe OSDU set up DUSSU, right?

50:56  
You'll remember that we don't ship those very often, but we definitely ship those in the beginning for the new OSS.

51:01  
As you come down, you will see here for 19H2 cumulative SAC, right?

51:07  
This is the LCU.

51:09  
Following that, you'll see the KB number.

51:12  
If you were to click on this, because this release has already gone live, you'll, it will take you to the release notes for this release.

51:20  
And then finally down here, you'll see TTGL time to go live, which means when is it going to be available to customers, Not internally for customers.

51:30  
And that tells you the date and the time.

51:32  
And if you were to look at a calendar, this would be the second Tuesday of the month of May in 2020.

51:37  
And 10:00 AM is our local time here.

51:40  
And so now let's go to the right and let's talk about what's here.

51:44  
So here's payload.

51:45  
And here you'll see this tells you payload, build, packaging and BBT.

51:49  
And so the first one, payload, this tells you how many bugs are in here.

51:53  
And because we have already shipped this, you see it says 111 out of 111.

51:57  
But right at the beginning, right, especially right near the check in deadline, you might see this as like 65 out of 111.

52:03  
And the next day it might be like 94 out of 111.

52:06  
As people are getting their fixes in, right, that number will go out, go up.

52:10  
So this is telling you how many are checked in and how many total are expected.

52:13  
If you were to click on this, this would take you to the payload report.

52:17  
I will not click on it and take you there.

52:19  
That payload report itself deserves another 30 minutes at least, but especially if you're a SUI or if you're in CFE, you will be looking at that all the time.

52:28  
You can also again get the payload report from here.

52:32  
This tells you the due date, tells you the check in deadline, and this up here tells you what package version we're on right now and what build version it's based on.

52:40  
So let's move over to build.

52:41  
This tells you what build there is.

52:43  
This is also great in we've already shipped this, but for example, for the next version, it might tell you, oh, there's a build that's churning or it might have a red, it might say something went wrong.

52:53  
We have an infrastructure incident.

52:55  
And if you were to click on this, right, every one of these is clickable and you'll have information here.

53:00  
It will tell you right up front and center, here's the incident.

53:03  
So if you're, you know, working on a fix and you're like, hey, I need my build on my package so I can verify you're like, where is it?

53:09  
You come to track it?

53:09  
You're like, oh, build failed.

53:11  
There's an incident, someone's acknowledged that they're working on it.

53:14  
Here's an ETA for the fix.

53:15  
Perfect.

53:16  
So this talks about build.

53:18  
If you click on this, this will actually take you to the build share and tells you the build number right here.

53:23  
Packaging again, same thing.

53:25  
It's telling you what has been packaged.

53:28  
Has everything been packaged?

53:29  
You might find that you know everything is checked in, but the build that was generated, right?

53:35  
It's still running.

53:36  
It's the last build is still running and so you might have a previous package.

53:41  
So when you come here, you're like, wait, so do I have the package that has all the fixes or does it have my fix, right?

53:46  
So that's really important for you to know.

53:48  
And then BBT, this is build verification test.

53:51  
And this basically gets run at every time we build.

53:55  
We do the build and we do the packages and it's basically making sure, you know, can we install it?

53:59  
Can the machine boot up again afterwards, right?

54:02  
Basic tests.

54:03  
Because if we can't install and we can't boot up the machine, we really shouldn't be wasting our time with this stuff anyway, right?

54:10  
I know we're right at 3:00.

54:11  
I'm going to try and go over just by a couple of minutes and I'll talk really fast.

54:15  
We'll move over.

54:16  
This is where validation starts.

54:17  
We talked about all these different types of validations, right?

54:20  
The app compat, I'll talk about Canary for 10 seconds.

54:23  
Canary is like an overnight, right?

54:26  
It's, it's kind of, if you were to look at all the app compat tests that we have and Canary will be like the most important.

54:32  
And we've distilled that into what can be run overnight and it'll give us like a quick Canary in the coal mine.

54:39  
You know, if those tests don't work, put the brakes on, something's wrong.

54:42  
If those tests pass, OK, let's keep testing.

54:45  
Let's do all our other efforts.

54:47  
We have self host, we have our MTPS.

54:50  
Every one of these, as you click on them, right?

54:52  
MTP, for example, will take you to the MTP reports.

54:55  
You can go and you can triage your issues, right?

54:58  
So it's fantastic.

54:58  
And it tells you what version MTPS were run on SUVP.

55:04  
This is testing with enterprise partners and you'll see over here it tells you 41 of the partners signed off.

55:10  
It's not mandatory.

55:11  
So we always hope for 100% participation, but not mandatory.

55:14  
And this finally is the sign off.

55:16  
During escrow week.

55:17  
Did we get sign off?

55:18  
And you'll notice until recently 19H2 was, you know, the the latest in market.

55:25  
And so CSD and feature team both were signing off.

55:28  
And then finally, this tells you, oh, it went to the world.

55:32  
And so it tells you where did it go?

55:33  
Retail.

55:34  
That's like the Wu SAS catalog and tells you, what did we publish?

55:38  
When did we publish it?

55:39  
If there's an incident, if it didn't get published, it'll show up right here.

55:42  
Bright red incident gets filed automatically.

55:45  
LSBT tells you, yeah, it went live on all our channels, right, Wu SAS catalog.

55:50  
So what's number four?

55:51  
Number four is our release notes that the documentation went live to.

55:56  
And then moving on here, Wise Lab and then here's post release so you can look at what are the incidents.

56:01  
Uh oh, we have an incident here.

56:05  
So looks like remote desktop and authentication issues after installing this KB incident's been filed.

56:11  
It's sev 3.

56:12  
It's on ENS.

56:12  
Uh oh, somebody in my team, they've acknowledged it.

56:15  
It was found through social and you can click through and you can see what's happening with this incident.

56:20  
And then here you'll see adoption and social.

56:23  
So this is a really powerful report.

56:25  
There are, there is so much built in here.

56:28  
There are a bunch of business rules that are providing a safety net, making sure we're doing all the right things.

56:34  
It is incredibly complex.

56:35  
I cannot do justice to this in a few minutes, but I'm hoping that by showing you can start using it and it doesn't seem as intimidating and you can get familiar with this.

56:45  
Yeah, I was gonna say my encouragement is this is the dashboard that we run our whole business with Lawrence know this, understand this this like the ramp team.

56:56  
I cannot give them enough kudos for how powerful this chart that you.

57:02  
I mean, I've been where this did not exist and we were tracking in spreadsheets and and you know, people would be manually monitoring and it would be like come in in the morning and be like, did my build finish?

57:12  
Oh, no, it failed at 11:00 last night.

57:14  
But like, you know, what build number are we on?

57:16  
Did it?

57:16  
What where are we at?

57:18  
Who knows?

57:19  
Nobody knows.

57:19  
And so this has been amazing.

57:21  
Like use this as your guiding, you know, principle of this tells me where we're at across every single point of inflection.

57:31  
Absolutely.

57:33  
I know we've gone over.

57:35  
I do apologize for that.

57:38  
Are there any questions?

57:39  
I'm happy to stay for a few minutes and take any questions or you're welcome to just send it to us.

57:44  
Reach out and we can answer any questions.

57:47  
Anything we can answer right now.

57:54  
No.

57:55  
Perfect.

57:56  
I'm gonna have a great weekend.

57:57  
Everybody have a great weekend.

57:59  
Thank you for joining us.

58:00  
I hope this was useful.

58:02  
I will send out a short survey and I would request that you please fill it out.

58:06  
I promise it will take about one minute to fill out.

58:08  
There's just a few questions and the reason we ask you to do that is to tell us if this was useful so we can keep offering it to other newcomers to our org.

58:17  
And also if you have any suggestions so that we can improve for the next round of newcomers.

58:23  
And just so you guys know, Namrath and I, we do not get paid based off of your surveys.

58:28  
It is just to let us know this is a true story.

58:33  
We, we really hope this was useful.

58:35  
Thank you for the time that you've given us and I hope this was helpful and please reach out as needed.

58:41  
Guys, we are really here to help you connect you.

58:44  
It is a very hard business to really wrap your heads around.

58:47  
It takes time.

58:48  
So be kind to yourselves.

58:50  
Don't beat yourselves up when you don't understand stuff and don't be afraid to ask.

58:54  
Absolutely thanks everybody.

58:57  
Bye, you guys.