**CSD 101 - Day 3 - Releases (B, C, OOB), SSIRPs, CritSits, Release Timeline, Security Workflow**

0:03  
And and as always, don't be afraid to ask questions in the chat and I can answer as we move along.

0:09  
So totally.

0:10  
All right, welcome.

0:12  
Day three.

0:13  
Yay.

0:14  
We're halfway there before we dive into the content for today, are there any questions from yesterday that we can answer?

0:26  
Any questions, any, anything that we talked about that that you want to clarify or didn't make sense?

0:37  
Nope.

0:38  
All right, let's dive right in.

0:40  
So we talked about this slide actually yesterday, but I've still brought it up today just to kind of help us ground ourselves in what we were talking about.

0:50  
These are some really large buckets and sort of a way for us to think about when we say we're servicing or we're keeping customers protected and productive.

1:00  
How are we actually doing that?

1:01  
What are we sending out to customers?

1:03  
These are the four buckets, security, non security fixes, features in sediment remediation.

1:11  
I know I, I briefly mentioned what each of these were yesterday.

1:14  
We're going to dive into the security portion and we'll see if we get to the non security portion today.

1:21  
We'll do our best.

1:22  
We'll see how we how we get how we get along.

1:24  
So let's talk about the security fixes.

1:27  
We have some principles.

1:28  
You know, on the previous page I said this happens on patch Tuesday or the second Tuesday of every month.

1:34  
And the terminology for that was people will say be released, right.

1:38  
And the reason they're saying that is what they've done is they basically take the calendar and look at the Tuesdays and that's how the weeks are counted.

1:47  
It's not by, you know, cause 'cause the, the way the calendar works, right, Of course it doesn't start on Monday every, every, every, every month doesn't start on Monday.

1:55  
And so it isn't really the weeks you see in the calendar.

1:58  
It's the B, it's the, it's the Tuesdays.

2:00  
So the 1st Tuesday is a week, The 2nd Tuesday, wherever it falls is B week and C&D.

2:05  
And of course sometimes you get an E week.

2:08  
And so because we ship security fixes on the second Tuesday, it's in the past Tuesdays, then we call it B week or people will sometimes say it's the B release.

2:20  
And then you might hear people say 4B or 5B and that's April, you know, the patch Tuesday for April or the patch Tuesday for May.

2:26  
That's the nomenclature.

2:28  
And so we have some principles for this, for this release and, and they're listed here.

2:33  
You know, our, our first one is that this is a security only release.

2:37  
The patch Tuesday is only for security fixes and that we always de risk this release.

2:44  
And I want to I want to expand on this a little bit.

2:47  
When we talk to customers, we know that taking updates, you know, that's not their job, right?

2:54  
Their job is maybe running a business, running a hospital, taking the update is to keep their system secure so they can continue to do their job.

3:01  
And so it's something they have to plan and something they have to do.

3:04  
And so it's, you know, customers, obviously we'll, you know, this, this isn't something that they're really part of their normal business, right?

3:16  
It's something we're asking them to do and just to keep their infrastructure running.

3:20  
And So what we tell customers is if you do nothing else, take the security fixes.

3:23  
That's the most important thing you can do to keep all your systems running and keep them secure.

3:29  
And so it's really important to us that we honour that.

3:32  
And we say, hey, if the only thing one and only thing you're going to do is take security fixes, we give them this one release.

3:38  
It is just security.

3:40  
Also, we want to de risk it, right?

3:43  
We want to be able to say this is the most stable and the most high quality.

3:48  
We don't want to give customers any reason to say, hey, I ran into a problem when I took that patch Tuesday or that B release.

3:57  
And man, I'm just, you know, next time I'm just not going to bother or next time I'm just going to wait a couple of months and let someone else work out the kinks.

4:05  
That that totally defeats the point of taking updates every month and being secure.

4:09  
And so we always want to de risk this release and make sure that it's security only.

4:15  
And if the highest quality, you know, we are a trusted partner.

4:18  
We want to continue to be a trusted partner and we want to help customers to be secure.

4:25  
And the other thing here as well is that this release goes to everyone in the world at the same time.

4:33  
And so it's really important that it is really high quality and that we're not causing problems, right.

4:38  
It's another reason to de risk it want to make sure that we have the highest quality and it's security.

4:43  
Only other thing to to know about this is that this is the only time of the month that we are allowed to reboot customers.

4:52  
And so if you have a fix that requires rebooting a a customer's device first, you will be asked why.

4:59  
And is there any way that you really, you know, can engineer it so you don't need a reboot.

5:04  
But if there is for any reason a reboot required for your fix, this is the one and only time every month that you can do that.

5:11  
And so you will find that you might have a non security fix and that speaks to the 4th bullet point that that requires a reboot.

5:21  
And because it does and this is the only time you can do that, you'll get an exception to put that non security fix into the B payload.

5:28  
But those are our principles for Patch Tuesday.

5:32  
And I will pause for a second in case there are questions before moving moving forward.

5:40  
And James, if you have anything to add on Patch Tuesday.

5:43  
Yeah, I was, I was just gonna add because people might ask, which is, well, what happens if we have a fix that has to go out after B that needs a reboot.

5:52  
An example is we have a, a SERP, which it will talk about, which is an active attack in the world.

5:58  
And yes, we, we have made the decision to do a second reboot before.

6:05  
It's rare and it's painful and it usually involves the CSDLT to make that decision.

6:12  
So it's not that it because it's very disruptive, very disruptive.

6:17  
So it's not that it can't be done, but our promise to the world is one reboot a month, which is painful enough as it is.

6:23  
But there are times when we have made the choice for various reasons to do it again.

6:29  
Yeah.

6:29  
And we'll talk about some exceptions for sure.

6:32  
Yeah, because you know, just the nature of our business, we do know.

6:37  
And from time to time we'll have those.

6:38  
And the other thing I put in the chat, which is where do we get all of these security fixes?

6:44  
And Namratha will dive into this quite a bit more, but I put a link that there is a team at Microsoft called Microsoft Security Response Center.

6:53  
And, and, and these security issues that go into B must come from them.

6:59  
And there's a, there's a strong strategic reason of why that is.

7:03  
Yes, Louis Wannacry and those big examples were examples of Serps.

7:07  
Those were active attacks in the world spectrum meltdown Wannacry.

7:13  
In fact, again, Namratha will get this.

7:15  
We in CFE or CSD are usually dealing with around 4 Serps a month.

7:22  
Absolutely.

7:23  
So they're not rare like they're happening all the time.

7:28  
And again, we'll we'll touch on all of this, but I just wanted to separate MSRC issues are what we call security.

7:36  
Everything else is non security, non security.

7:39  
Absolutely.

7:41  
All right, if there's no other questions about Patch Tuesday, let's talk about the non security fixes and you know, and the monthly update that happens for that.

7:50  
And I want to talk a little bit about a recent decision that was made as well, right?

7:54  
I think that would help.

7:55  
So if you can't ship non security fixes on the B release or in patch Tuesday, well, you need some other time that you can do that, right?

8:04  
And so that time is the C release or the D release.

8:08  
And I will give an update on where we stand with D releases as well now.

8:12  
And so the idea behind this, I'm going to take a step back.

8:17  
Remember yesterday we talked about consumers and commercial customers.

8:21  
And so consumer would be like my mom, you know, for the most part, I think a lot of consumers don't really notice and don't really care when we send out updates, right?

8:29  
They're just kind of my mom, you know, does Facebook and looks at recipes and video chats with my kids and, you know, updates get download in the background and she reboots when she's told to.

8:37  
Our commercial customers, however, are not like that.

8:41  
First of all, they have many more devices than just the one little laptop, right?

8:44  
They have many times thousands and 10s of thousands of devices and they have businesses that they're running, right.

8:52  
And So what they will do is they need to be able to plan.

8:57  
They need to know, oh, updates are coming, this is when they're coming.

9:02  
And then how am I going to deploy them?

9:04  
And again, they're not just going to blast them out, you know, to 70,000 devices in their enterprise, right?

9:09  
They're going to do it in, in phases or in circles, right?

9:13  
So they really need to be able to plan and be thoughtful about this.

9:16  
And so we want to give them that predictability.

9:19  
And I know I touched on this slightly yesterday, but that's why you have like patch Tuesday, the second Tuesday of every month, 10:00, right, Redmond time.

9:27  
It's to give them that predictability.

9:29  
They can plan to this cadence, they know it.

9:31  
They know today when you know patch Tuesday is going to come out for July because they just go look at a calendar 2nd Tuesday, 10:00 OK.

9:39  
And so similarly for the non security fixes, they need that predictability.

9:44  
And so we said, OK, we're going to do a release on C and a release on D and that's the third Tuesday and the 4th Tuesday.

9:53  
And this is only non security fixes and you cannot reboot customers.

9:59  
This is why, right when you have a non security fix that does require reboot and there's absolutely no way to work around it, you then get an exception to put it into the patch 2 to the B release.

10:11  
Because on the C or the D you can't reboot customers, right?

10:15  
And it's only non security.

10:17  
You can't put security fixes into this.

10:19  
And so those are the the predictable release trains for non security fixes.

10:25  
Now, the reason that we had C&D for many, many years, we actually just had C So we had second Tuesday, that's patch Tuesday and 3rd and and the third Tuesday, which is the non SEC, the C release.

10:37  
And do you remember that line right when we went into Windows 10, right?

10:40  
So we started with Windows 10 and as is common when an OS first comes out, there's a higher number of non security fixes that we need to do.

10:49  
And so we were doing that, right?

10:51  
And we were trying to stick with this non SEC fixes go out in the C release.

10:55  
And as you'll notice, Windows 10 we released every six months, right?

11:00  
Not like these Windows 7, Windows 8, which came every two 3-4 years.

11:04  
Well, now every six months we've got this new release and we've got, you know, this whole new slew of non security things that we need to get out.

11:12  
At the same time, we still got to keep servicing everything that's already been out there, right?

11:16  
And So what we found was wow, we were struggling a little bit with this.

11:19  
And so we actually separated out to C&D.

11:21  
We said, OK, C non security fixes for all the down level, the real down level, not just 8-1 and earlier.

11:27  
And D was invented the 4th Tuesday to say OK, non security fixes for the latest in market because that's the one that has the highest volume of non security fixes, has a lot of churn.

11:38  
And so let's just give ourselves a little bit of breathing room.

11:41  
And again, it's still predictable.

11:42  
You know it's coming on the 4th Tuesday at 10:00, right, predictable.

11:47  
And so we have that on Monday of this week.

11:49  
So just a couple of days ago we made a decision to standardize all the non security releases on C again.

11:58  
And so you will see that in the past, yes, yay in the past you'll see C&D.

12:04  
But from next month, from July onwards, you will find only C is the non security fixes.

12:12  
I do also want to touch slightly on the timing and you and I'm and I know that I've said this before, but it's so important.

12:20  
Predictability is very important for our customers.

12:23  
With patch Tuesday, we do not have any wiggle room.

12:27  
It needs to go out on the second Tuesday at 10:00.

12:31  
And I'm really not exaggerating when a a few years ago, you know, I told you that SSD really invested in the world class service.

12:38  
And a few years ago, when we would send out the releases, right, the actual code, we would also send out release notes.

12:45  
And the release notes tell you, OK, you know, this is for this OS and these are the kinds of things that we've fixed in this, you know, And so again, someone like my mom would never read it, but you know, IT professionals and enterprise admins, they would read those release notes.

12:59  
They, they do care about them.

13:00  
And like 1005, right, the release notes wouldn't be shipping out at the same time as the packages because we had some kinks in our system.

13:07  
And 10:05, the phone would start ringing.

13:09  
Where are the release notes?

13:10  
I see content.

13:11  
Where's the release notes you know or if we ever had any publishing delays and you know something fell over on the publishing side and content didn't publish for five 1015 minutes.

13:21  
It was delayed.

13:21  
There'd be phone calls.

13:22  
So it's very important the predictability so there and there really is no wiggle room on Patch Tuesday now for the C&D releases.

13:29  
Third Tuesday 4th Tuesday still 10:00 Redmond time.

13:35  
There is some wiggle room and I say that because one, you know, we don't, we don't send it out to the whole world.

13:43  
It's not, it's not a required update.

13:45  
Whereas the security, you know, everyone should take it, it's required.

13:49  
But we, we are careful about that, right.

13:52  
You don't want to fall into this pattern where every month it's like, oh, well, you know, we need a little more time.

13:57  
We're going to release on the third, you know, on, on the Wednesday and then the next month it's like, oh, Thursday.

14:02  
And then the month after that it's back to Wednesday and then you're kind of on a Tuesday.

14:05  
Now you're really back to being really unpredictable.

14:07  
And our, our commercial customers really do need that predictability.

14:10  
So we, we have a little bit of wiggle room.

14:14  
We can move, you know, to the Wednesday or the Thursday of that week if we need.

14:18  
But it's not a decision that we just make the drop of a hat.

14:21  
It's a decision that happens with our leadership team, right?

14:25  
So our, our suite directors from CFE, right, the team that does the fixes for the most part and our suite director from the pub, the pipeline team, right, SSD is there.

14:37  
We have, you know, and, and we really are comp, this team is made aware.

14:41  
And so we really take that decision seriously.

14:44  
We have a little bit of wiggle room, but we're trying not to exploit that.

14:47  
We're really trying to make sure that we are a trusted and predictable partner to our customers.

14:52  
So just a little bit about the timing there.

14:55  
Any questions?

14:59  
All right, let's talk about exceptions because there are always exceptions.

15:03  
Yes, so so James mentioned this slightly and I I want to dig into it a little bit.

15:10  
So we talked about security fixes, non security fixes, predictable release schedule for those right.

15:14  
And sometimes, you know, people talk about them as release trains.

15:17  
It's the same terminology, but we do have some exceptions.

15:21  
And the two big things here are Serps and crit sets are incidents.

15:24  
So a SERP, this is, you know, these are security incidents.

15:29  
If you've worked at a team in Microsoft outside of CSD maybe, and you were working on a new product, you might recollect that for every new product you need to have a cert plan, right?

15:40  
And it basically is a software security incident response plan.

15:46  
And it's something that gets logged with MSRCMSRC is the Microsoft Security Research Centre.

15:52  
It's an organization that sits outside of CSD.

15:55  
It is a, it is a Microsoft organization, but they sit outside of CSD, one of our strongest and tightest partners.

16:02  
In fact, we have a person in our organization, Kaushik, who sits in CFE, who is a dedicated liaison because we interact with them so much.

16:13  
Though of course people across the organization work with MSRC, but but we have such a tight relationship with them and our leadership and their leadership meet every quarter as well.

16:24  
And so if you're building a new product, you would have logged a cert plan.

16:27  
Well, these are products that are already in market.

16:30  
Well, it's still important to have an incident response plan.

16:33  
And the reason is every so often what's going to happen is a security vulnerability will be made public.

16:39  
And that means that customers and of course also people who are wanting to exploit it will be made aware of it.

16:46  
And that will happen before we have had a chance to actually release a fix for it.

16:52  
And that's a SERP.

16:54  
And the goal behind a serp is that we really need to be really quick in assessing the damage, minimizing the damage and then figuring out how we're going to fix it.

17:05  
James mentioned we have about four Serps every month.

17:08  
And you know, and if you ever attend central ship room or maybe your local ship room, you will definitely for sure be hearing about Serps.

17:17  
And so that, that can tell you also that we do have a SERP playbook and we know how to deal with them because it, this is not a one off thing.

17:26  
So we need to know how to take care of these.

17:28  
It's something that we do very well.

17:30  
There's a well oiled process.

17:32  
A syrup will be declared by MSRC.

17:35  
They will, they will give information that they have on it.

17:38  
You know, what has been declared publicly, who has declared it?

17:41  
You know, what do they know about it?

17:43  
How damaging do they think it is?

17:45  
And based on the information they have, you know the severity level of it, then they will inform CFE and they'll spin up a bridge or a call and then the CFE folks will get involved on that PM and suite both again, try to assess, figure out if we can mitigate or minimize the damage, and then figure out when we're going to fix it.

18:06  
Our goal typically is to fix it via the next train or the next, you know, release a vehicle the next patch Tuesday.

18:14  
Anytime we do something outside of our, you know, release trains out of outside of our planned releases, it, you know, it is disruptive.

18:23  
It's disruptive to us because you're now having to spin up more work streams and having to do all that work while in parallel all the regular release trains need to still keep going.

18:32  
It's also disruptive to our customers, right?

18:35  
Because anytime you release something that's outside of that predictable cadence, right?

18:39  
Especially for a, which is we then, hey, not only are we releasing it out of band, but it's going to go to everybody and it's going to have a reboot, right?

18:47  
Super disruptive because all the admins in the world are going to see it pop up on their consoles.

18:52  
What is that?

18:53  
What's going on?

18:54  
It's a security thing.

18:56  
I got it deployed quickly and it's going to be another reboot on top of my, you know, the Patch Tuesday reboot I took this month.

19:03  
So super disruptive.

19:05  
So we do try to put it on the next B, the next train every so often.

19:11  
We really can't wait for the next train.

19:13  
And that is where we will do an out of band or UB.

19:16  
People will say UB release, out of band release.

19:19  
But again, it is a last resort.

19:21  
It's not something we're keen to do and certainly something that we take very, very seriously.

19:28  
Yeah, absolutely.

19:31  
So let me talk about what happens when we have crit sits or incidents.

19:36  
These are not security issues.

19:38  
These are non security issues.

19:41  
Crit sit is something that an enterprise calls in and it's a critical situation.

19:45  
I can't function, my business can't operate because something has happened.

19:51  
They they do need to actually have a contract to be able to call in with the crit sit.

19:55  
It's not again not something that you know, random user in the street is going to call into.

19:59  
There is a well oiled process for this.

20:01  
Our partner for this is CSS, not MSRCMSRC only deals with security.

20:06  
So crits that will come in through CSS customer calls, CSSCSS that engages with us, they will file it into our bug database.

20:14  
There's a certain way of marking it and, and again, the teams will triage and the first thing is to assess and then to de escalate or, you know, figure out how we can mitigate it.

20:25  
Sometimes it's, you know, it, it, it's a work around that we can offer them.

20:30  
Sometimes it's we, hey, we need to really throttle, you know, this update and and until we have a fix for it.

20:38  
So de escalating does not always mean that we need to actually release another fix, right?

20:42  
It could be any number of ways that we can de escalate and then we are going to fix it.

20:49  
The goal again is to fix it via predictable train, you know, not, not an out of band release, but every so often we really do need to issue an out of band release.

21:00  
It's our last resort because again, that's very disruptive to us and very disruptive to customers.

21:06  
In this particular case though, the out of band releases do look different.

21:10  
With Serps, I mentioned it goes to everyone and it reboots the world.

21:13  
With out of band release for a crit sit or an incident, it will go to catalogue.

21:18  
We'll talk about publishing channels in a little bit and, and why that's important that it's catalogue.

21:22  
But it basically it goes to a place where you as a customer have to go pull it.

21:26  
It's not being pushed to customers.

21:29  
Whereas you know when we do an out of band for SERP, it's being pushed to every customer.

21:33  
With an out of band for a crit sitter, an incident, we put it on catalogue.

21:37  
You as a customer need to go pull it because we want to minimize the disruption.

21:42  
Now, they're always exceptions to exceptions too.

21:45  
So I have a great story about that.

21:48  
If are folks aware of what the Super Bowl is so that there's American football has this event every year and it's the Super Bowl.

21:56  
I will confess that I don't actually watch it, but I hear the commercials are fabulous.

22:01  
But it's a really big event in that they have a very, very large viewership and a lot of money is on the line and a lot of exposure is on the line.

22:11  
And so many years ago, 3-4 years ago, the folks who the NFL, right, So the folks who do the Super Bowl, they use these Surface devices and the Surface devices are right there in front of where the person who's doing the commentary is.

22:27  
And then that person's on TV.

22:29  
So the device is visible to like all the millions of people watching the Super Bowl.

22:32  
And they said, oh, we have a problem.

22:34  
So it was a crit said, we said, great, we can fix this for you super easy.

22:40  
Here's a fix and it's on catalogue.

22:43  
You need to go pull it and put it on your devices.

22:45  
And they said, ha, we can't do that.

22:50  
And we said, what do you mean?

22:51  
Like you go get the fix and you put it on all your machines like you would any other fix.

22:57  
Well, it turns out that their method of deployment was not quite sophisticated.

23:04  
And so they really were not able to go grab a fix from catalogue and go deploy it.

23:09  
They really needed to be pushed to them, but there was not a way for us to push it to just the NFL machines and no other machines.

23:17  
And so we ended up shipping this out of band release to the world for a non security for a crit set because the PR impact and the the the negative, you know, impact of seeing these devices, millions of customers are going to be seeing them on TV and that they're not functioning correctly was so high.

23:41  
So that was our exception to our exception.

23:42  
It's one of my favourite stories.

23:45  
Yeah.

23:46  
James, did you have anything to add here?

23:49  
No, I've been putting a whole bunch of different links and things for everybody.

23:55  
If you want to go dive deeper, we do have a whole wiki on how to work with CSS.

24:00  
We have a whole wiki on how to work with MSRC.

24:03  
Those are really our two big partner teams, which is, you know, your non SEC coming in through CSS, through customers and then MSRCS security.

24:13  
There are other paths, but those are our two main teams.

24:15  
Umm, and so there are links there.

24:18  
Umm, you know, I, I will tell you this.

24:22  
We always do as Numratha said, we try to follow this golden path.

24:27  
And I did also put the central shiproom link.

24:31  
I would encourage all of you, don't be afraid to join those ship rooms and observe how this all works.

24:40  
It will literally sound like gibberish the first couple times you join because they're moving like lightning speed.

24:49  
But every month I, I don't even know if I can say a month that went perfect.

24:57  
And so we had a month like last year.

25:00  
We don't know if we've ever had a month.

25:03  
And so they are constantly making really intense decisions and conversations.

25:09  
And here's the problem.

25:11  
How do we work there?

25:11  
What do we do?

25:13  
And so you'll really get a good sense of it's not this super smooth process every month at all in terms of because there are always issues whether we found regressions and we need to fix them.

25:25  
There's an active attack that's going on.

25:27  
There's a team that needs this because they're shipping like surface.

25:30  
We have this all the time.

25:32  
So there are always these interesting exceptions that I swear are every month that come in and there's yeah, and there's real customers on the other entities and there's real implications.

25:45  
And so the discussions are very thoughtful and, and you know, this is where we go back to our principles, right?

25:51  
Keeping customers protected and productive, right?

25:55  
The principles around Patch Tuesday, this is when not this is when security items need to go out.

25:59  
This is when we can reboot the world, right?

26:02  
And, and that helps to ground us and to guide us, right?

26:05  
And you'll find that if you attend ship rooms, people will come back to these principles over and over and over.

26:11  
And when the discussion is sort of spiralling out of control, people will go, OK, wait, what is our guiding light here, right?

26:17  
Our principles when you go back to those.

26:19  
So you'll find that a lot.

26:20  
And I do encourage you like James to attend ship room.

26:24  
If you are in CFE or SSD or CPC, all these teams have a have a local ship room.

26:32  
I'm not aware of test base having a local ship room.

26:35  
They might, I'm not aware of it.

26:37  
That's something to something to find out about.

26:40  
And and you know, the local ship rooms will vary a little bit, right?

26:43  
So the CFE local ship rooms probably sound pretty similar, right.

26:46  
SSD local shiprooms sound a little different, right.

26:48  
I've been to those and they have an operational right, a tech OPS meeting with talk about these operational things they need to do and then they have a planning and how all the work that they are doing towards the monthly releases.

27:02  
And so it's gonna be a little bit customized to your area, but they're really a great way to learn about the business.

27:09  
And I agree with James, the the first time you walk in any ship room, and honestly, the first week you walk in any ship room or you dial into any ship room, man, it's a hard place to be because you're just like, what are they talking about?

27:20  
They're talking it.

27:21  
It almost feels like people are talking out of thin air or out of the blue.

27:25  
And the reason is because ship rooms, if you haven't, if you're new to Microsoft, or if you haven't, you know, been in ship rooms before, ship rooms are not designed to have like entire context built into them every time.

27:36  
They're meant to be an ongoing conversation.

27:39  
So it's almost like, you know, where we, we were talking on Monday and it's like nothing, you know, like we just pick it up right, right where we left off on Tuesday.

27:47  
And then on Wednesday, you pick up right where you left off on Tuesday.

27:50  
And so every day you're just picking up where you left off the previous day.

27:53  
And so when you first walk in, you're like, what is going on?

27:56  
They just seem to be randomly talking about these weird topics.

27:59  
But for the people who attend regularly, they then learn that there's a rhythm and there's a method and, and then you kind of fall into that.

28:08  
So I do encourage it and don't be discouraged when you when you attend the first time and it kind of seems bizarre.

28:15  
Yeah.

28:15  
And and what I would add to that is that it, it really is a great place to learn the business because they really do talk about that at that level.

28:27  
They're not at specific problems.

28:28  
They're not at specific.

28:29  
It's the business.

28:31  
How do we operate, how do we think, how do we drive?

28:34  
Yeah, absolutely.

28:37  
I will touch on incidents.

28:38  
It's on this slide.

28:40  
We'll talk about incidents more later too.

28:43  
Incidents, this is not a tip.

28:45  
Not always.

28:46  
Sometimes it can be not always a customer calling in, right.

28:50  
Chris said is enterprise customer called CSSI have a problem critical situation.

28:55  
An incident is when we have released an update and something has gone wrong.

29:00  
We hope.

29:01  
And our goal is that we release it and we find it, right.

29:06  
I mean, of course, our first goal is don't even release something that causes an incident, right.

29:10  
But the reality is that we we do sometimes cause regressions or cause problems.

29:16  
And so then our goal is can we detect it and can we detect it as fast as possible, right?

29:22  
Because if we can detect it and we can do that as fast as possible, we can mitigate and take care of that incident before it impacts too many customers.

29:29  
That's so that's, that's, that's definitely very important to us.

29:32  
And we'll talk about incident management hopefully on Friday.

29:36  
But responding to an incident is typically also, you know, something that we try assess, mitigate and then we try to fix that the, the, the long term issue in the next predictable train.

29:52  
But every so often that may not be possible and you will need an out of band release.

29:56  
A browser example was a great one.

29:58  
It happened a few months ago.

30:00  
Is that right, James?

30:01  
When the, when the websites for the UK government stopped working, whole slew of websites stopped working, right.

30:08  
And so people who needed to go into the websites to like maybe submit a claim or, you know, for, for welfare or for anything, or for people who even use that websites to do their jobs, suddenly none of those websites were accessible.

30:22  
It turned out when we shipped a fix, we were trying to actually close a security vulnerability.

30:29  
We ended up closing it way too far and accidentally shutting out these sites.

30:36  
And so that was an example of an incident that we caused.

30:39  
Now that was an incident that we noticed and got reported very loudly by many customers.

30:45  
And so that was one where the only way to fix it was really to do an out of band release.

30:50  
There was not a way for us to mitigate other than that.

30:52  
So, yeah, all right, let us let us move forward.

31:00  
Let's talk about our release timeline for a moment.

31:04  
I don't expect anyone to memorize this, but I'm going to speak to it.

31:10  
And then you will find that as we move forward, I will keep coming back and talking about this.

31:16  
And so I will spend a few minutes to explain this.

31:20  
And you'll notice here that this is Monday through Friday, right?

31:23  
There's multiple weeks represented here in this timeline.

31:26  
And you'll notice here I've called out, hey, this is a patch Tuesday.

31:29  
And again, you know it because of the way the calendar works, right?

31:32  
That's not always the same date every month, but we know it's the 2nd Tuesday and a week later is the C release, right?

31:38  
The non security release.

31:39  
Well, every month because of how the calendar works, our schedule is a work back from the patch Tuesday date.

31:46  
And so you'll notice that that everything is always calculated as a minus work back.

31:52  
So what happens?

31:53  
Well, let's see, right, Right before we release, we need to sign off, right?

31:58  
That means we're done, right?

32:01  
But actually I'm going to work.

32:02  
I'm going to go left to right.

32:03  
That might be easier.

32:05  
We are going to take a look at here's all of our security issues.

32:09  
Here's all of our non security issues.

32:12  
And we're going to talk about the workflow in just a few minutes, but we're going to, you know, we're going to triage, we're going to figure out whether we need to fix them.

32:19  
What's the right fixes?

32:20  
There's a whole slew of work that happens here.

32:22  
Sometimes this work takes a few days, Sometimes this work can take months and months.

32:28  
Even SRP sometimes can take months for us to work through.

32:31  
Spectre and Meltdown were great examples.

32:33  
And so this where you see it's a little bit open-ended.

32:36  
This represents that this could be a week, a month, two months, four months.

32:41  
But at some point you're going to say this security fix or this non security fix, it's going to go out in 7B, that's patch Tuesday of July or it's going to go out in 8C.

32:51  
You know, the non SEC release in August.

32:53  
You're going to determine once you know that you go look at that date and you look at all the work back for that date, right?

33:00  
And that tells you, hey, this is the check in deadline, right?

33:03  
It's about I think 33 days before the release for patch Tuesday, right?

33:08  
After the check in deadline, you'll notice there's a DTP week.

33:10  
That's the depth test pass week.

33:13  
This is the week where typically, as you noticed, the check in deadline was right here.

33:18  
All the fixes have been checked in.

33:20  
And this is the week where bills are getting made, packages are getting made, and developers are doing, they're submitting DTP requests and they're doing validation of their fixes.

33:33  
And so this is where they're testing.

33:35  
Oh, you know, everything that I fixed actually works correctly.

33:38  
All the different, you know, combinations and permutations of that, the negative testing, etcetera.

33:45  
That's what's happening during this week.

33:46  
The following weeks are there two of them, MTP week one and MTP week two.

33:51  
And that stands for monthly test pass.

33:54  
And So what is the difference?

33:55  
Because you know, we just said hey, they were testing department test pass.

33:58  
Why we now have another two weeks of testing.

34:01  
Well, you can kind of think of this as integration testing and a lot of teams people talk about integration testing.

34:06  
This is where what we do is we have all the fixes, right?

34:11  
So if this was a 7B schedule, all the fixes for 7B for that particular OS version get put on the device and then they all get tested together, right?

34:19  
All these test cases are run with all these fixes living together on that device, which means that if my fix is doing something to mess up your fix, this is when hopefully we are going to find out about it.

34:29  
Right.

34:31  
And MTP also covers actually a slew of things we have, we're going to talk about validation later, but this isn't just test getting run in some lab.

34:39  
There's actually four or five activities.

34:41  
And so we have a whole section validation where we'll we'll get into that.

34:45  
But I would also like to take this chance to say, do we have Louise on the line?

34:50  
Yes, I am here.

34:52  
Louise in the house.

34:53  
Woop, woop.

34:55  
So he on the PM side owns the the MTP and DTP work.

35:00  
And so Louise, would you like to chime in now or maybe we'll be talking about validation.

35:06  
Sure.

35:06  
I can just say something real quick is that everything you said is absolutely correct.

35:11  
We work very closely with all partners, you know, across Microsoft.

35:15  
For example, just today we had each us in office that, you know, we brought up to the feature teams to be able to to fix them because they were found in MTP.

35:25  
So it is extremely important for us to work across Microsoft to be able to, you know, do all this testing.

35:32  
And to Narrata's point, all this integration testing to make sure that we reduce the risk of having post release incidents that happen after we ship it.

35:41  
Because the earlier we can find that, you know, closer to DTP rather than NTP gives us more time to prepare so that we can have a very clean B release.

35:51  
And just to give you an idea about the magnitude of it, we run over 200,000 test jobs.

35:59  
That's not test cases, that's test jobs.

36:02  
A job can have multiple test cases in it, you know, and this happens every month.

36:09  
So it is a significant amount of work that happens across the teams.

36:12  
And we open box with all of the duos across all of CSD and they work in tandem to make sure that we fix issues prior to be released.

36:21  
So it is a significantly important work that happens every month and I'm really proud of the team come coming together every month to get it done.

36:31  
Yeah, and, and yeah, thank you for being the PM driving that.

36:37  
Happy to help.

36:38  
It is.

36:38  
It is absolutely mission critical.

36:40  
I, you know, cannot emphasize that enough.

36:43  
Yeah.

36:43  
And, and there's a whole slew of activity here.

36:46  
Yeah, very important for us to get this right.

36:49  
And you will find that during this time, right as we're, especially as we're getting closer and closer towards that B date, you will find that this is where every team's SLA is getting ratcheted up, right?

37:05  
The closer you get to the B release, right?

37:06  
When things go wrong earlier, it might be OK, you know, business hours, then it's like OK, slightly longer hours the closer you get to the B release.

37:15  
It's weekend work if it's needed, right?

37:18  
And so MTP is an example of a team where, you know, as we're getting closer and closer, as you're getting closer towards the end of MTP week two, if things are going wrong, if you know, if they're finding issues of teams are needing to address them, right, the urgency gets kind of kicked up.

37:34  
I also want to talk about the concept of churn really quickly, which is that, you know, all this testing is happening.

37:41  
There's three weeks, right, where we're doing all of this testing.

37:43  
Well, our hope is of course, that there are no bugs, right?

37:46  
But that's not always going to be the case.

37:48  
There are going to be issues.

37:49  
And the goal of our testing is to find those issues, right?

37:52  
We don't want to find the issues after we release over here.

37:55  
We want to find them here.

37:56  
That's what the test period is for.

37:58  
And So what you'll find is that as issues are getting found and as Louise mentioned, they're getting logged, people are triaging, they're working with the test team.

38:06  
You know, they, they might be saying, hey, having trouble with getting logs or you know, hey, can I, can you help me with the repro, etcetera.

38:12  
But then there might come a time where you go, hey, you know what, there's a real problem.

38:16  
I need to make a code fix to actually address the bug that was found.

38:20  
And that's where you'll have churn.

38:23  
So because you're past the check in deadline, you're going to go to some, you know, your local ship room and your central ship rooms to get approval right for that churn.

38:31  
But that's what churn refers to, which is that past the check in deadline, but before the release, there was some issue and you need to now make another check in, which will then of course trigger another build, another packaging and then more testing, right?

38:46  
This would be where you coordinate with Luis and his team and you say, hey, you know, we need to hold some validation or we need to restart some validation, right?

38:55  
So that's something important to know.

38:57  
And MTB week one and week two, kind of a very easy way to think about it if you're kind of trying to distinguish between those two weeks.

39:03  
The goal always by the way, is to have everything ready for MTP week one.

39:07  
That's when all the testing gets kicked off MTP week two is often thought about as a rerun week.

39:12  
You know, during week one we found bug fix was checked in.

39:16  
You can rerun the test in Week 2.

39:18  
During week one there was a problem with our infrastructure and test couldn't run.

39:23  
You can rerun it in, you know, in week two.

39:24  
So often people think of it as a rerun week, but as always, life is not so clean.

39:31  
It's not so black and white and or so clear or easy.

39:34  
And so sometimes you'll find that, hey, we, you know, things were more complex.

39:37  
We needed more time.

39:38  
Tests actually started part way through MTP week one.

39:41  
Maybe they started on the Wednesday or Thursday and they bleed over into week two.

39:44  
So not always so clear, but that's the idea.

39:48  
And James, were you going to say something?

39:49  
Yeah.

39:50  
I was going to add in that kind of another key piece to the puzzle of all of this, which is whenever we receive a security MSRC issue, it comes in as an ADO bug.

40:03  
It comes in with an SLA date.

40:06  
And that SLA date is basically a ticking time of when we have to have that fix out to the public before that date.

40:16  
A lot of times it means that the Finder who can be a researcher, an outsider, could be Google, are going to go public.

40:24  
With the vulnerability.

40:26  
And so a lot of times what you'll find is this drive to make sure we're getting all of the right MSRCS into the releases before this SLA date.

40:37  
So you'll hear a lot about the SLA date, which drives what content kind of goes into what month, and we'll talk about that security workflow in more detail.

40:47  
Absolutely, Yeah.

40:50  
So all right, let's let's let's see if we can make our way to the end of the timeline.

40:53  
So we've done all this validation.

40:55  
Hopefully we found all the issues.

40:57  
We've, you know, we've had all the appropriate churn to address all of those issues.

41:01  
And now we're at the end of MTP week two, everything's done and we have our final what we think we're going to ship with our shipping packages and escrow is the idea that this is when it's basically time to dot the IS cross the TS, right.

41:15  
That's the idea is that you have all of your final shipping packages in hand and now you're doing, you know, hey, kind of make sure we close out all our bugs, make sure nothing, nothing is left untriaged.

41:28  
Make sure that you know, the publishing team is lining up everything on the SSD pipeline team side to, to keep it ready so that it can go live at the right time.

41:37  
You know, all those activities are happening.

41:39  
That is the goal of escrow.

41:41  
And of course with the Friday being the sign off that you know, everyone signs off and says yes, we're good to go for the latest in market CSD signs off, but also the feature team sign off for everything that's down level.

41:53  
So not 8-1 and earlier, but the the real down level, right?

41:57  
That's, you know, CSD does the sign off for it.

42:00  
This is the hope behind escrow.

42:02  
You will find however, that sometimes we are churning into escrow week.

42:07  
It could be a couple of reasons.

42:09  
For example, we might find a bug during validation right here, right in the Friday, right at the end of MTP Week 2.

42:15  
You need some time in escrow week to you know, people will be working over the weekend, but you might need some time in escrow week to address it.

42:20  
Sometimes it's late breaking, you know, changes like a late breaking SERP.

42:26  
We identified a SERP sometime right here and you know, by the time we figure out the fix, we're into the escrow week and, and returning now again, we try to be as as least disruptive as possible.

42:38  
And so if we could put that SERP fix in the next B train, we would try, but sometimes you can't, right?

42:44  
It's, it's too risky, right?

42:46  
It's too severe.

42:47  
And so then we'll make the calculated decision of is it better to kind of churn in the escrow week?

42:53  
Because remember, our principle is to de risk our release.

42:56  
So should we churn during escrow week or is it better to put this in the next B release?

43:03  
And so then it'll, you know, the discussion will be what is the risk if we're churning an escrow week for this B release, you know, we're putting this release a little bit at risk versus if we let the SERP wait until the next be released.

43:15  
How exploitable is it?

43:17  
How severe is this SERP, Right.

43:18  
So that's an example of a discussion that would happen, right?

43:22  
You know, James said, hey, every month or something or the other that comes up, it's an example of a discussion that would happen.

43:27  
So while escrow should be a quiet week, it's not always a quiet week, right?

43:32  
It can be, in fact, it can be quite a tense week because remember I talked about the urgency ratcheting up.

43:36  
It's at the highest in escrow week.

43:38  
Yeah.

43:40  
And then Friday is sign off.

43:41  
This is when we say we're done and then everything is staged and ready to go live on the Tuesday for Patch Tuesday.

43:48  
Interesting thing to note is that for the C release, everything is the same.

43:54  
All the work for the C release is done on the same timeline as the B release, which means you don't get a week later check in deadline.

44:00  
This is your check in deadline for B&C.

44:03  
These are your validation periods for B&C.

44:05  
This is your escrow & off for B&C.

44:08  
And so we hold the C for a week longer.

44:11  
Now I will say that every so often we'll find an issue and we'll need to churn right the C release where the issue is in some non SEC fix.

44:21  
And so we can let the B release go out on time because it has to, but we can churn right during escrow and maybe even during this week to get that C release just right.

44:32  
But, but, but the idea is that you are in the same timeline now when we did have D releases that obviously would be further out here that did have an offset check in deadline, etcetera.

44:44  
But since those are going away, we won't go into that.

44:47  
Yeah, I was going to say the other thing about that was different about DS was they didn't have the MTPS and the same type of validation programs.

44:55  
So it's it's actually better and less confusing to get rid of it.

45:01  
Yes.

45:01  
So thankfully it is.

45:03  
But also know that for for the latest in market that we call CBE still often where current branch, the validation process for it is different.

45:14  
And so it is very key when when Namratha says down level and it's separating out the active branch and the latest in market, everything else is down level follows this pattern.

45:26  
The other two you'll hear often about flighting and you'll hear this often.

45:32  
And flighting is a very active branch concept that they've been using for a long time.

45:37  
We've been trying to integrate it down into the other once they're released to market branches.

45:44  
But know that there's kind of those three things.

45:46  
The active branch was active development, the CB, which is the latest in market.

45:51  
And then everything else is, is the way I break it up in my head.

45:55  
Yeah.

45:55  
And when we talk about validation, we will touch on that more too.

45:58  
I think that is helpful to talk about.

46:00  
Yeah.

46:02  
All right.

46:02  
If there's no questions, let's see, we have about 10 minutes, right.

46:06  
Let's see if we can talk about the security workflow.

46:10  
I'll do my best.

46:11  
And and prior to Cow Shake, James was our MSRC liaison, right?

46:14  
Yeah.

46:15  
So James, please chime in.

46:17  
So we mentioned earlier that MSRC is our partner for security issues.

46:23  
And so MSRC is, is this is the place where all the security vulnerabilities are tracked and they, this is the team that interacts with all the entities outside of Microsoft relating relating to security vulnerabilities.

46:42  
So what happens?

46:44  
A Finder, this is a person who finds an issue outside of Microsoft and reports it.

46:48  
We call them finders.

46:49  
A Finder will find some vulnerability, right?

46:52  
And these finders could be anybody.

46:54  
It could be a person who just enjoys doing this kind of work and it's just kind of doing it in their free time.

47:02  
It could be an actual company.

47:04  
Google actually has a set of people who this is their job.

47:07  
This is what they are paid for, right?

47:09  
And it could also be just because this is what happens.

47:12  
It could also be somebody who's out there doing it but doesn't always have the best of intentions, right?

47:17  
So, you know, it kind of it's, it's, it's, it's a wide range of folks when we say Finder, but whoever the Finder is, they will find a vulnerability and then they will report it to MSRC, right.

47:28  
MSRC has a, a, a, a method and a process for people to, to bring these things into them.

47:33  
MSRC will log it in the database called Gray Matter, which I always think is a really cute name.

47:39  
And it will have an Ida case ID.

47:42  
And this will be unique for every security vulnerability.

47:45  
So no two MSRC cases will have the same ID.

47:49  
There will be an SLA and this is what James was talking about.

47:53  
Typically I think the SLA is 90 days.

47:55  
Is that right James?

47:57  
Or is it 120?

47:58  
It's typically 1/21/20 except for browser, right?

48:04  
Browser gets the 90, everything else 120.

48:08  
That's right.

48:09  
And so how about 20 days?

48:10  
Yeah and that's the default unless the Finder has come and put a different date because a lot of the time they will disclose them at conferences like Black Hat or Blue Hat or these kind of security conferences.

48:24  
And so that's what's more pressure on us at times yeah.

48:27  
And that's where the third bullet comes in negotiations because the Finder, you know, typically it's 120 days.

48:33  
And, you know, and especially if it's a Finder who interacts at MSRC regularly, they know this, right?

48:38  
And so they'll report something and they know there's 120 days, right?

48:41  
That's the SLA by which Microsoft has to release a fix for it.

48:46  
But an example that we had last year, this Finder said, listen, I understand there's 120 days SLA, but there's this huge conference coming up, and this is my keynote speech.

48:56  
Like I can't give you 120 days, you know, and then of course MSRC will try to negotiate, right?

49:03  
And sometimes the negotiations go in our favour and sometimes they don't.

49:07  
MSRC spends a lot of time building these relationships with these finders, especially the ones that are repeat kind of they they submit repeatedly.

49:16  
I was going to say repeat customers, but that doesn't sound right.

49:19  
Like they submit repeatedly.

49:21  
And so they definitely spend time building these relationships and, you know, then they can have these negotiations and hopefully be successful.

49:30  
So that's on the MSRC site.

49:31  
So now you'll notice we have an MSRC bot shout out to Louis and his team.

49:35  
Woop, woop.

49:36  
They take what's in the Gray, the, the Gray matter.

49:39  
And then what they do is they move it over into our database and you and you know, and there's this little arrow there.

49:45  
But really what's happening is that the, the Gray matter database is where the, the, you know, that's sort of the, the, the source of truth, right?

49:55  
What this bot is really doing kind of 32nd summary.

49:58  
And Louis can share a lot more if you guys are interested.

50:01  
What this bot is doing is it's going in and it's saying, oh, there's a new case in Gray matter.

50:06  
I'm going to open one in, in our database in our ADO.

50:10  
But anytime something changes on the Gray matter site, it will also bring that over because remember that that's where the source of truth is.

50:16  
This also means that the SLA that's discussed is in Gray matter and it gets pulled over to us.

50:21  
So, you know, if you go in and you go, no, we need more time and you change that SLA and our ADO, it doesn't mean anything when it really what's in Gray matter is the source of truth.

50:31  
And so, you know, there's just a heads up for anyone who's in CFE and is thinking about that.

50:36  
So the what the bot does is it takes that one case, brings it over into our ADO, actually opens it up as a task group.

50:44  
And what you'll see underneath that is one item, one bug, one item for every OS that's in support.

50:52  
So if you remember on day two, I think we talked about all these different OSS.

50:57  
So you can imagine now there's one bug for every OS.

51:00  
Windows 10 version 2004.

51:02  
Oh, no, actually the active branch now will be 20H2, right?

51:05  
20H2, the active branch right 2004 latest in market 19091903 all the way down to Windows 7 SP one and are embedded.

51:17  
You know, OS is everything that's in support.

51:19  
Louis, how many bugs is it per task group nowadays?

51:23  
It's 1414, Yeah, 14 on, on, on.

51:29  
I, I believe that the number I, I, I need to find the latest number.

51:33  
But I think on average we process between or we create or update between one and 2000 ADO items per day.

51:43  
Yeah.

51:43  
And, and what's interesting is really important, right?

51:45  
Because again, information's coming over from Gray matter when they update it.

51:49  
Yeah.

51:49  
And with security issues as a platform, you are guilty until proven innocent.

51:55  
So, so it could be that, hey, this security volatility doesn't apply to a bunch of operating system, but you have to go and prove that and then close those bugs.

52:05  
Yeah, absolutely.

52:06  
And that's where the analysis and applicability comes in, right?

52:10  
So this is where the folks typically in CFE, every so often in CPC, right?

52:14  
Because something comes in against the update stack maybe or update client, they will get that vulnerability report.

52:20  
And then, you know, the bot will open bug for every OS and support and they need to go figure out how bad is this vulnerability?

52:28  
Is it really a vulnerability?

52:30  
How bad is it?

52:31  
How severe is it?

52:32  
How exploitable is it and is it applicable to all these different OSS?

52:36  
It is not the finder's job to tell you that.

52:40  
The Finder might say, you know, I found this on RS5 on Windows 10/18/09.

52:44  
Great.

52:45  
It doesn't automatically mean it applies to every Windows 10 OS.

52:48  
It also doesn't automatically mean it doesn't.

52:50  
And this is where you have to figure it out.

52:53  
And so sometimes you'll find that, you know, that security vulnerability applies across the board.

52:58  
Sometimes you'll find it applies only to Windows 10, sometimes you'll find it only applies to RS3 and above, so not all Windows 10, because you know, that component was introduced in RS3.

53:08  
So they really have to do that analysis.

53:11  
Something that's important to call out a vulnerability.

53:15  
Again, not just the OSS in support, but also the active branch.

53:18  
Because whatever we're going to ship next, we need to make sure that's secure too, right?

53:23  
Very important.

53:24  
You can't say everything that's in market is secure, but the next one that comes out, well, you know, who knows?

53:30  
So that's very important.

53:31  
That needs to be made secure too.

53:32  
So we have to analyse as it's a problem in the active branch and the next one that's going to come out.

53:37  
And the last thing I'll say here, and I know we only have two minutes, I'll be really quick.

53:41  
Once we determine it really is a vulnerability, you know, it's a legitimate vulnerability and we determine all the OSS that it applies to, right?

53:49  
Whatever those OSS might be, all or some, then when we decide to fix it, we have to simultaneously ship, You'll hear that called SIM ship.

53:59  
We have to do that.

54:00  
So you can't say there's a vulnerability and I'm going to fix it on RS345 and above in 8B.

54:08  
That's the past easy of August.

54:09  
But for everywhere else that it's applicable, I'm going to fix it in nine B, right?

54:13  
You have to SIM ship.

54:14  
And the reason for that is once we issue a fix for a security case, for a vulnerability, the minute it goes out, there are people that take our fixes, our updates and they start reverse engineering them, right?

54:27  
And you don't want to put customers in a position where there is a vulnerability and we are not providing them with a fix for it.

54:35  
We're providing a fix for some OSS, but not others.

54:38  
No, our, our mission and our goal is protected and productive.

54:43  
And so we can't say, well, we knew about it and all these OSS, but we only kind of gave you the fix for some OSS right now.

54:48  
And the others, well, you know, they'll kind of come later and also number out that like SIM ship doesn't mean just OSS.

54:55  
It could mean across other products at Microsoft.

54:58  
It could also mean, it could also mean other companies like Google and Amazon.

55:03  
So SIM ship is a powerful principle and it, and it means we will SIM ship wherever in the it's never needed.

55:12  
It is applicable.

55:13  
Yep.

55:13  
And that could be some and that could be some really hard coordination at times.

55:18  
Yes, I agree.

55:19  
I think, you know, browser is a great example, you know, where the browser team has the the interaction with Adobe, they have the interaction with Chrome, right.

55:28  
That is some ship got a coordinate all your partners, you know, so it's very, very important.

55:34  
And and you'll see here I've said else we SERP and I'll take 10 seconds to say really quickly about that because I know we're right at 3:00.

55:41  
If we have a security vulnerability that we identify hits, for example, all the OSS and we ship the fix for it for all the OSS except one, whether maybe that's accidentally, we didn't ship it or intentionally.

55:55  
Either way, we have now Serped ourselves, which means that the vulnerability is out in the wild and the customer does not have their hands on a fix or the ability to get a fix.

56:04  
So really we shouldn't be serving ourselves.

56:06  
Don't do it.

56:09  
We're right at 3:00.

56:10  
So I will stop if there are questions.

56:13  
That's the worst type of syrup.

56:15  
It's true.

56:16  
The worst one, don't hit yourself in the foot.

56:20  
I will you will be having a Carlos conversation.

56:24  
If we self-serve and it's also just so much pain that we're inflicting on our customers and ourselves and it just it's the worst feeling.

56:31  
It really is.

56:33  
I know we're over time, I will stop and I will stop the recording.

56:36  
If there are questions, I am happy to hang out for about 5 minutes or 10 minutes and take questions.

56:43  
But I will officially stop the recording now and folks are are are welcome to drop off and we'll see you tomorrow.

56:50  
See you tomorrow, everybody.