Audio file

2020-05-13_TeamMeeting_process_TTPs.m4a

Transcript

00:00:12 Speaker 1

Usual suspect.

00:00:17 Speaker 1

It's my friend [Name Redacted].

00:00:19 Speaker 4

Oh, hi, [Name Redacted].

00:00:20 Speaker 1

What's going on, [Name Redacted]?

00:00:22 Speaker 2

It's a beer.

00:00:23 Speaker 4

Sorry for the confusion earlier, I just got off the phone second ago with [Name Redacted]. That was a fun, wide-ranging conversation, I told him.

00:00:33 Speaker 4

He can't use my name.

00:00:34 Speaker 3

That's right.

00:00:34 Speaker 4

Because I'm in the process of interviewing with Facebook.

00:00:44 Speaker 4

But we had plenty to talk about anyway.

00:00:53 Speaker 2

OK, so we have meeting in a second. Let's just go make sure we catch everybody else.

00:01:01 Speaker 2

Team meeting.

00:01:07 Speaker 2

And which one of us is running this? But you know whatever.

00:01:10 Speaker 1

That's you.

00:01:29 Speaker 2

Well, looks like you got a couple of minutes to wait.

00:01:40 Speaker 2

And this is my last meeting of the.

00:01:42 Speaker 2

Day which is good.

00:01:44 Speaker 1

So you think?

00:01:46 Speaker 2

OK.

00:01:49 Speaker 2

Yes, I know it's never the last meeting.

00:01:51 Speaker 1

Never the meeting. It's it's the meeting before the last meeting. It's the penultimate meeting.

00:02:02 Speaker 2

We'll be OK.

00:02:08 Speaker 1

I just. I just want to do this before.

00:02:10 Speaker 1

We get the meeting started.

00:02:15 Speaker 2

The small, cute person I heard data.

00:02:18 Speaker 1

You did? No, he's he's gone.

00:02:22 Speaker 1

My, my, my COVID fighting spaceship.

00:02:27 Speaker 4

Nice. I like that.

00:02:30 Speaker 5

Sick background.

00:02:42 Speaker 4

Yeah. So one thing I realized while I was talking to [Name Redacted], I was trying to find.

00:02:47 Speaker 4

This in exchange about Facebook censoring the morning in America ad where somebody that I was connected to on LinkedIn, who works in policy at Facebook, who I think a lot of us know trying to remember who it was. So I was looking through everything.

00:03:05 Speaker 4

And apparently, whoever that is in policy at Facebook blocked me.

00:03:13 Speaker 4

Which is, you know, maybe not a good sign, but.

00:03:19 Speaker 1

Getting blocked by.

00:03:20 Speaker 1

People you might be interviewing with is.

00:03:22 Speaker 1

Typically not a good sign.

00:03:26 Speaker 2

I don't know that could be fun.

00:03:29 Speaker 4

Well, it could make for an interesting conversation. It would be good practice in contrition conflict resolution.

00:03:39 Speaker 4

Conflict resolution.

00:03:46 Speaker 2

All righty.

00:04:03 Speaker 2

Oh, hey, [Name Redacted].

00:04:07 Speaker 7

Your friends.

00:04:12 Speaker 4

I don't think he's even. He may not even be public on any platform anymore.

00:04:21 Speaker 2

And note 8, we'll give it a.

00:04:23 Speaker 2

Couple of minutes.

00:04:26 Speaker 2

I'm going to do some screen sharing just.

00:04:29 Speaker 2

For the heck of it.

00:04:33 Speaker 2

Because I can.

00:04:46 Speaker 2

OK.

00:05:04 Speaker 2

We're going to assume that we've probably got most of the people we need.

00:05:08 Speaker 2

And the rest were just wondering when we need them.

00:05:15 Speaker 2

OK.

00:05:18 Speaker 2

So [Name Redacted] was going to join us. I'll just double check.

00:05:25 Speaker 2

See if he's actually around.

00:05:34 Speaker 2

How many screens?

00:05:38 Speaker 5

Do you have?

00:05:39 Speaker 5

Can you check you might have different permissions on the slack channel. See if you can do it at here or channel notification for the team meeting. Cuz I can't, but maybe people just didn't see the.

00:05:53 Speaker 5

Alert. You know, I sent two reminders, but I mean ****. Maybe that's maybe I need more.

00:05:58 Speaker 7

Yeah, I would do that here.

00:06:01 Speaker 2

OK.

00:06:03 Speaker 2

Up here.

00:06:10 Speaker 7

And if you don't have permissions, let me know. And [Name Redacted], if there are specific like admins for that group, let me know and I'll tell [Name Redacted] and we'll get that fixed.

00:06:12

OK.

00:06:23 Speaker 2

Yeah, we definitely need to get that.

00:06:24 Speaker 5

Fixed. OK, I'll.

00:06:26 Speaker 5

Ping Ping 8 Right now for me in Australia, perfect rest of us, yeah.

00:06:34 Speaker 2

OK.

00:06:36 Speaker 2

Well, we're 5 minutes in. We've got.

00:06:40 Speaker 2

Nine of us.

00:06:41 Speaker 2

That's enough.

00:06:43 Speaker 2

OK, meet ups, change the format slightly. We're going for 1/2 an hour of Team coordination and then half an hour training.

00:06:51 Speaker 2

Just so we don't split what we're doing this week.

00:06:55 Speaker 2

We gotta talk. So we're going to talk about what we're doing, how we're doing it, how we're structuring, where we're doing it.

00:07:02 Speaker 2

So we've got a few people in.

00:07:06 Speaker 2

So any newbies?

00:07:12 Speaker 2

I'm staring at you, [Name Redacted].

00:07:15 Speaker 2

You knew.

00:07:20

Hi, yeah.

00:07:23 Speaker 2

So we have a slide for anyone who's new every week just to say this is where you find everything. So I'm [Name Redacted]. I coordinate the team.

00:07:33 Speaker 2

You can also see [Name Redacted] and [Name Redacted] in here.

00:07:41 Speaker 2

Come grab us if you need anything. If you look in the team slack right at the top, there's the description. There's a link to a readme.

00:07:52 Speaker 2

You can get from that README to most everything else you need. It lists how to get the tech, who to sign up, who to who to tell.

00:08:00 Speaker 2

Big book.

00:08:01 Speaker 2

It's basically our team manual and there's all the.

00:08:04 Speaker 2

Texts we're using.

00:08:07 Speaker 2

OK. And what we.

00:08:08 Speaker 2

Do OK, thank you background.

00:08:12 Speaker 8

I'm I'm I'm a researcher from Israel. I've been recruited by [Name Redacted], I've. I've been researching this information.

00:08:29 Speaker 8

Naturally, like everyone since 2016, even a little bit before the US elections and looking at the situations here in Israel and broad.

00:08:50 Speaker 2

You'd be a good person to have, yeah.

00:08:54 Speaker 2

Thank you. OK, status update for this week. Deliberately blank because we're going to talk about where we are.

00:09:06 Speaker 2

Let me do some.

00:09:06 Speaker 2

Of this.

00:09:11 Speaker 2

[Name Redacted] and [Name Redacted] are going to be working with me on this this week, so this is our road map of where we how we get through tactically from getting an alert through to doing something about it and all the systems and pieces we use. So stuff comes in, we make sense of it. We basically write it up in hive.

00:09:32 Speaker 2

Collecting data and objects into Deccan Wisp GitHub.

00:09:37 Speaker 2

[Name Redacted] code, other pieces of code enrich it, come back to slack.
00:09:42 Speaker 2

And some of MISP to report that. To counter that, do something about it.

00:09:48 Speaker 2

OK. But bottom line is we're not doing this for fun. We're trying to find.

00:09:57 Speaker 2

In the disinformation space that we can spot and make a difference to.

00:10:04 Speaker 2

That our position in CTI uniquely allows us to do.

00:10:11 Speaker 2

We sat down and sketched out.

00:10:14 Speaker 2

What we've been doing recently, so this this is basically the day-to-day stuff.

00:10:20 Speaker 2

Stuff comes in. We shove it through tech, we try to do something about it. This is the thing we've been.

00:10:26 Speaker 2

Trying to build.

00:10:28 Speaker 2

But actually there's levels way above that.

00:10:32 Speaker 2

So at the very, very top level is what the cogset collab, which is the team that we seed it the CI league team from.

00:10:41 Speaker 2

So it's a little nonprofit that we built to support.

00:10:48 Speaker 2

And build out the text and processes for.

00:10:56 Speaker 2

Volunteer Community group disinformation responses. So we've all come out of this, infosec this idea of using information security principles, practices on disinformation. So basically the idea is to build a response system. We've got a heck of a lot of stuff heading for us.

00:11:15 Speaker 2

We've got a.

00:11:15 Speaker 2

Lot of volume, a lot of different actors, a lot of different types of actors, a lot of different locations.

00:11:22 Speaker 2

And there is just getting worse. We've got, you know, the anti vaxxers joining up with the right wings. We've got somebody doing for money in Australia, feeding stuff through the protesters over here, pushing back out to other countries.

00:11:40 Speaker 2

And we.

00:11:42 Speaker 2

Just got to build these responses.

00:11:45 Speaker 2

It's like joined up, so strategically that's kind of the point.

00:11:52 Speaker 2

And it's to do this.

00:11:57 Speaker 2

For COVID, which is a carrier.

00:12:00 Speaker 2

For an awful lot of.

00:12:04 Speaker 2

This information at the moment like today I was sat on a call talking about how.

00:12:14 Speaker 2

Terrorist cells and.

00:12:19 Speaker 2

Organised criminals, we're starting to use disinformation.

00:12:23 Speaker 2

Starting get into campaigns. It's just like it's everywhere.

00:12:27 Speaker 2

I it's.

00:12:30 Speaker 2

How do we build this stuff and how do we create this network of people who can do this so?

00:12:40 Speaker 2

I I know that I I do most of the talking in these meetings.

00:12:45 Speaker 2

Be because, quite frankly, I'm the one that remembers to write the slides, or rather, [Name Redacted] kicks me to remember to.

00:12:50 Speaker 2

Write the slides.

00:12:53 Speaker 2

But this is about all of us.

00:12:55 Speaker 2

Is about us as a network professional. Putting this together, so when I say great another no disinformation person, it's like.

00:13:03 Speaker 2

The more disinformation people can get into this community of intersect responders building out this, how this works together, how we build this information CDI the better.

00:13:15 Speaker 2

Because we need this.

00:13:18 Speaker 2

Operational you wrote this [Name Redacted]. It's yours.

00:13:24 Speaker 1

And usually it's elected.

00:13:26 Speaker 1

It's mine, but I did lick this slide.

00:13:32 Speaker 1

The the operational part is is the part that often gets neglected, and it's the part between the big strategic goals of we're going to do a thing and the the tactical level of here's what we did. There's a middle layer there of of translating what we're going to do to how we're going to do it.

00:13:51 Speaker 1

And so part of this is that, you know, once we develop this body of knowledge, we need to have a standardized process.

00:13:58 Speaker 1

For training new members and for keeping up the proficiency of existing members. Because tactics, techniques, and procedures change, adversaries change the way that things happen. Change, and so it's it's important to train new members in how we do things.

00:14:19 Speaker 1

That it's equally important to maintain the proficiency of existing members.

00:14:24 Speaker 1

But if we're going to do that, we have to maintain kind of an operational understanding of campaigns across verticals. And what I mean by that is you know, anti VAX misinformation may be different than 5G. Misinformation may be different than COVID information or they might be using all the same tactics.

00:14:44 Speaker 1

But if we can look at campaigns, regardless of their intended audience and their their intended influence, we can make sure that we're not missing any big points that we could affect.

00:14:59 Speaker 1

And once we see those, we should be able to update the body of knowledge based upon the changing situational realities. The way that misinformation was done prior to Facebook and and Twitter. Or you know if you will prior to the 2016 elections is not the way it's being done now. And so I can tell you that.

00:15:19 Speaker 1

Even professionals that do this for.

00:15:20 Speaker 1

Living in inside of military forces are very confused as to why we're seeing this sudden resurgence of what led to it, because they didn't have a fundamental understanding of social media and social networks in in the Internet age as they did in in the pre Internet age.

00:15:41 Speaker 1

So updating the.

00:15:41 Speaker 1

Body of knowledge is important and then we need to engage with the various communities.

00:15:49 Speaker 1

So that we can help them gain greater cognitive and system resilience and and response. Right now everything happens kind of right of boom. So after an incident, everybody runs around with a chicken like a chicken with their head cut off and and tries to figure out what happened and how did it happen and how should we respond well.

00:16:09 Speaker 1

If you let people know that, hey, these things are possible in whatever your line is, and you should plan a response or at least have discussions about who should be in the room for the response, I think you'll you'll greater success in in preventing these things.

00:16:27 Speaker 2

Yeah, we're going to head into tactical, but one thing to note about disinformation is that our team is.

00:16:35 Speaker 2

Slightly different from the rest of CTI in much of CTI, somebody can come in, drop a report in.

00:16:45 Speaker 2

You're dropping an IC and you're done.

00:16:48 Speaker 2

In disinformation it it's not like you can do it in five seconds it there's a degree of work in tracking and tracing.

00:16:57 Speaker 2

A degree of time involved. It's a different.

00:17:03 Speaker 2

I'm not, yeah.

00:17:03 Speaker 9

Requires contextualization.

00:17:07 Speaker 2

Yeah, it's.

00:17:10 Speaker 7

Can I? This is. Yeah, I wanted to just ask a question before we move to the tactical. As far as the operational.

00:17:20 Speaker 7

I don't have the depth of experience that everybody else does. You know, I I do a lot of independent work on my own.

00:17:28 Speaker 7

And you know, coming into the the COVID disinformation space with a lot of the targeting with the healthcare, that's sort of how I got catapulted into it just for context for everybody.

00:17:43 Speaker 7

As far as the operational, I'm looking at the participant list here and I'm just trying to catch up with everybody else.

00:17:54 Speaker 7

I wanted to share I I stepped up to help with the vetting team because I do have a background in Osment.

00:18:04 Speaker 7

Just so you know, there's some mumbling going around that.

00:18:07 Speaker 7

There are people.

00:18:10 Speaker 7

There's journalists in this in the in the larger CTIA League.

00:18:16 Speaker 7

And I just wanted to share that.

00:18:20 Speaker 7

To be mindful of that, I don't know if this is something that is of a concern for this particular group.

00:18:28 Speaker 2

We we have.

00:18:29 Speaker 2

Solutions coming on that.

00:18:31 Speaker 7

OK, I I didn't wanted to share that.

00:18:31 Speaker 2

So one of the thing that's that's about, yeah. So one of the things that's about to happen is we've had a smaller active channel created for us.

00:18:43 Speaker 2

And that's part of the discussion today and that's part of why we've just carved out.

00:18:48 Speaker 2

A discussion with all the people who were going to turn up.

00:18:53 Speaker 2

So this was a basically there were there are people who will just keep coming back and you're it.

00:19:00 Speaker 1

The the other thing I'll add just very quickly is there. There's absolutely no egos in this group. Nobody's an expert on this or to be.

00:19:09 Speaker 1

A solved problem.

00:19:10 Speaker 1

Some of some of us have been working bits and pieces of this a little bit longer, but there's no such thing as a stupid question and you're all in here for a reason. So.

00:19:20 Speaker 2

We're building this thing as we're flying it.

00:19:22 Speaker 2

I mean no.

00:19:23 Speaker 2

Yeah, your work, your work is good. I've seen what you.

00:19:24

You have.

00:19:26 Speaker 2

Do and it's.

00:19:31 Speaker 2

We built this stuff. We we are in here because we know we don't have the answers yet.

00:19:37 Speaker 7

Yeah, thanks. Thank you.

00:19:37 Speaker 2

And this is a place we can build out those answers we can build.

00:19:40 Speaker 2

Out those pieces.

00:19:43 Speaker 7

You know, I I'm just very worried and very careful because of what you do and it's so critical. I I'm just concerned about if if journalists are in, I don't know who else is in. Right. So I wanted to just be careful and I wanted to say that out loud and name it so good.

00:20:02 Speaker 7

I'm glad that that's already on your radar. Thank you.

00:20:05 Speaker 3

Yeah, just just to briefly.

00:20:06 Speaker 2

We were actually talking that we.

00:20:09 Speaker 3

Sorry. Yeah, just to briefly jump on that we have.

00:20:15

Like we've had.

00:20:17 Speaker 3

Not specifically general, whatever, but security has been an issue that we.

00:20:25 Speaker 3

Have sort of looked at, particularly because we have a a what I call a huge lurker problem right now it's 65 to one ratio between lurkers and participants.

00:20:41 Speaker 3

You know that's never good. So what? What we decided?

00:20:47 Speaker 3

In a smaller meeting of principles was that we would create a.

00:20:53 Speaker 3

A smaller inner group for people who are.

00:20:58 Speaker 3

Trusted and sort.

00:20:59 Speaker 3

Of have.

00:21:01 Speaker 3

Demonstrated that they are active participants and they would need to know and are not just there to lead to information or anything like that. So there's.

00:21:13 Speaker 3

The existing channel, that too many people have access to.

00:21:19 Speaker 3

Is literally going to have nothing that isn't public. It's going to be shifted to helping white.

00:21:28 Speaker 3

Level of information the.

00:21:31 Speaker 3

Triage group will be amber and to get into that, you all sort of have to be vetted.

00:21:40 Speaker 3

Not onerous, but it's, you know, we won't be letting any.

00:21:44 Speaker 3

Doing the same thing so.

00:21:46 Speaker 3

Thank you for raising a specific concern that we should lookout for, and absolutely this is something.

00:21:53 Speaker 3

That we are addressing.

00:21:55 Speaker 2

And the thing I was about to say was that we were talking about needing somebody on the team to do that.

00:21:55 Speaker 3

That's it.

00:22:01 Speaker 2

Vetting and basically run an HR function for us.

00:22:06 Speaker 2

And there was one name just kept coming up.

00:22:09 Speaker 2

Hi, [Name Redacted].

00:22:11 Speaker 7

I got you.

00:22:13 Speaker 2

OK. Thank you.

00:22:20 Speaker 7

Don't. Don't lick me, right?

00:22:26 Speaker 2

OK. So right, let's let's move to the next bit, so tactical.

00:22:36 Speaker 2

So basically these are these are things we've been doing in channels. So we've been doing two things, tactical and execution. We've actually been running response, but we've also been building the things.

00:22:46 Speaker 2

So creating the team, creating the processes, creating the tool sets we need.

00:22:52 Speaker 2

And you've seen us, you know.

00:22:54 Speaker 2

Build these, iterate these. Adapt these.

00:22:58 Speaker 2

Just to do this thing where you start with that, that was the diagram way back here of the alert through to action. So it's alert the new staff.

00:23:10 Speaker 2

Make the instant data, so get instant data available for people to analyze and to get to the other teams. So one of the reasons that.

00:23:19 Speaker 2

We don't use Google Docs, apart from the fact it it makes.

00:23:25 Speaker 2

[Name Redacted], come out in hives. Is that by putting artifacts into Hive and MISP?
00:23:33 Speaker 2

That becomes accessible to the dark Web team and the other team leads.

00:23:39 Speaker 2

Which means that if they have URLs of interest that we we hit, or if we have URLs that they hit, we can share and share across.

00:23:49 Speaker 2

We also analyse so a lot of this is doing things like tracking data back to origin, but it's also finding trends. It's finding the pressure points. We can make a difference at.

00:24:00 Speaker 2

So find the Super spreaders.

00:24:03 Speaker 2

Find the the hashtags are good. Find the the endpoints, find the end events, find the things we can.

00:24:10 Speaker 2

And and then start affecting. So do those mitigations, there are mitigations built into CT I already.

00:24:18 Speaker 2

So the fact we have the registrar so we could take down the banks, that's.

00:24:22 Speaker 2

An easy one.

00:24:23 Speaker 2

But there's also the counter set that we've built back in [location redacted].

00:24:30 Speaker 2

It's a mess.

00:24:31 Speaker 2

But there's work to be done in just listing out the counters we can use.

00:24:36 Speaker 2

So into the big book we add in per.

00:24:40 Speaker 2

Artifact per tactic, per technique. The counters going to talk about that a little bit further down.

00:24:48 Speaker 2

Recommending defenses.

00:24:51 Speaker 2

So before we get incidents and we know some of these are going to happen, we know the events are coming through. We know what people are likely to.

00:24:57 Speaker 2

Do it's like we know damn well.

00:25:00 Speaker 2

That we've got a massive anti vex campaign coming.

00:25:04 Speaker 2

Ahead of any COVID-19 vaccine.

00:25:09 Speaker 2

We're already watching the right wings and the the anti vaxxers gearing up towards it.

00:25:14 Speaker 2

We know there are going to be events, possibly nation state, amplified events coming ahead of the next waves.

00:25:22 Speaker 2

We we we can make decent decent sized guesses at what's coming for coming for us and start defending ahead.

00:25:30 Speaker 2

We we can.

00:25:30 Speaker 2

Start taking down some of the Ms. type.

00:25:35 Speaker 2

Can I say the word creep I can.

00:25:37 Speaker 2

Say the word creep.

00:25:39 Speaker 2

But we know it's making.

00:25:41 Speaker 2

Money off the back of some of.

00:25:42 Speaker 2

These Mets we know.

00:25:43 Speaker 2

He's going to keep trying again.

00:25:45 Speaker 2

We we can see the gun naps writing the the the reopen. They're going to keep coming. They're going to keep trying to sell T-shirts on whatever the whatever it is, is is going on. We we know where the new domains list is. We can sniff that.

00:26:00 Speaker 2

So it's getting ahead of this, this this is getting left a boom on this. And [Name Redacted], you've been in this again educate the masses.

00:26:09 Speaker 1

Yeah. So one of the things that comes up often is when you talk about misinformation, kind of the de facto response by by larger groups, IE the government is we'll, we'll just put it in the educational system, which is great if if you want to treat the next generation. But what do we do with all the?

00:26:29 Speaker 1

Generations that are no longer, you know, going elementary, middle and high school.

00:26:34 Speaker 1

And so there really needs to be kind of a public campaign kind of like we see in the US Now with the, you know, home alone together from the national Ad Council, where we educate the citizenry on how do you look at things critically, how do you ask questions? How do you verify sources? I know I posted in.

00:26:54 Speaker 1

Very well written article today on LinkedIn about somebody that was looking at the pandemic video.

00:27:01 Speaker 1

And what I liked about it wasn't just the results, it was that that particular journalist went through their thought process and the questions that they asked themselves to try to validate or or invalidate the claims in that pandemic video. And so I thought it was very well done. So educating the masses.

00:27:22 Speaker 1

Educating not just the school aged children, but the adults that might otherwise be the consumers of this misinformation.

00:27:30 Speaker 2

Yeah. And the other thing is, as we build these processes tool set with, it's useful to a bunch of other teams. We're basic prototyping, we've we've got NATO has set up his own lisps. Now they're talking to the UN today. We'll probably talk them into doing it too. We'll end up with these things linked around the world.

00:27:53 Speaker 2

And we're just like watching us.

00:27:56 Speaker 2

That help us? So that's a tactical thing.

00:27:58 Speaker 8

If I can ask a quick question if.

00:28:02 Speaker 8

If I can also ask about.

00:28:05 Speaker 8

You mentioned the mainly domestic actors, but we've seen also that state actors are ramping up. We've seen the US and China on both sides escalating their information campaigns. There are other state actors that.

00:28:26 Speaker 8

Might use the situation to Inter.

00:28:29 Speaker 8

And I've seen the you also have U.S. government and it is on our on our team. So how do we relate to you know state actors in this sense.

00:28:43 Speaker 2

Definitely track we we're more than happy to track state actors up to now. Most of the activity.

00:28:48 Speaker 2

Has been non state, quite frankly just dealing with the reopen UPS has taken a lot of our time. It's.

00:28:57 Speaker 2

Do we have the resources to track it? We've set up a China instant list. Just keep it. Keep running tracking.

00:29:06 Speaker 2

But if we've got.

00:29:08 Speaker 2

The resource is set up to do it. We'll do it.

00:29:11 Speaker 2

If we are best placed to make that difference.

00:29:16 Speaker 2

If there are other teams doing that already.

00:29:16 Speaker 10

And then.

00:29:20 Speaker 10

Sorry, I was wondering, did I hear in your question [Name Redacted] concern about being able to effectively track US state operations when we have U.S. government officials in the channels? Was that your question or no?

00:29:32 Speaker 8

No, I I was. You know, when you raise it.

00:29:37 Speaker 8

It's it's really some kind of a of a concern, but no, I was asking more broadly about if, if that's even in the scope of our interest because the the.

00:29:52 Speaker 8

Focus was not really on the domestic stuff.

00:29:55 Speaker 10

Got it.

00:29:56 Speaker 2

No, the the the scope.

00:29:58 Speaker 2

The the thing that's been limiting us so far has been the amount of resource, the amount, the amount that we've got set up already. So it's taken a while to get.

00:30:08 Speaker 2

The tech set up.

00:30:09 Speaker 1

The other thing the the other.

00:30:11 Speaker 1

Thing that's limited us is.

00:30:14 Speaker 1

Nobody knew who was responsible for dealing with this, right? Everybody thought that they, you know, everybody wanted to get funding for it, for research, but then nobody wanted to be responsible for actually doing anything.

00:30:25 Speaker 1

Think about it. And so getting people in the room to discuss, you know, what could you actually do if you had the know how? And then, you know, what do you need besides to know how to do it? Is is a challenge. But at least now we've got the right people.

00:30:38 Speaker 1

In the room to have those discussions.

00:30:40 Speaker 2

Well, in, in terms of what CTI does, there is no objection to tracking state disinformation campaigns.

00:30:47 Speaker 2

In fact, they're interesting. They're fun. They're huge.

00:30:51 Speaker 2

UM.

00:30:52 Speaker 2

It it just, it can be a resource suck.

00:30:56 Speaker 2

So we have to know that we can, it's that.

00:31:03 Speaker 2

Alert to action. Think we have to know that we can take action that's meaningful, that we can actually have an effect of for the amount.

00:31:09 Speaker 2

Of effort we put in.

00:31:12 Speaker 2

That's the only thing that matters.

00:31:14 Speaker 9

Product management problem.

00:31:16 Speaker 2

Yeah. Can we do something useful? What we got?

00:31:19 Speaker 4

So I have a question. Does that mean?

00:31:22 Speaker 4

That it that we wouldn't.

00:31:25 Speaker 4

Put the effort into tracking state sponsored disinformation campaigns. If we didn't think we could do anything about them.

00:31:36 Speaker 1

I don't think that I don't think that.

00:31:37 Speaker 2

So one of the things we can do is to pass the information off to somebody who can do something.

00:31:43 Speaker 1

So we.

00:31:43 Speaker 4

Well, what if nobody, I mean.

00:31:46 Speaker 4

Go go ahead, [Name Redacted].

00:31:48 Speaker 1

You know, we've briefed several governments and several multinational agencies. [Name Redacted] talked to NATO earlier this week. I know we've talked to Canadians. I know we've talked to representatives of the US government. I know we've talked to the press.

00:32:08 Speaker 1

I I think we're interested in tracking everything because we want.

00:32:11 Speaker 1

It all to stop, right? I.

00:32:13 Speaker 1

Mean I I I've spent. Go ahead.

00:32:16 Speaker 4

So I guess I'll just be a little bit more specific here, I think.

00:32:20 Speaker 4

That by any objective definition, big proportion of the president's Twitter feed would count as a state sponsored disinformation campaign. But I think that there's.

00:32:33 Speaker 4

There's a cold, hard reality that we probably can't do anything about it. And then there's also the fact that.

00:32:40 Speaker 4

Actually like a database that lists that as a state sponsored disinformation campaign.

00:32:46 Speaker 4

Is going to be an uncomfortable thing for certain government employees to be working in the same building as if you.

00:32:54 Speaker 2

Yeah, we were on a separate meeting about that this morning. It's OK. The the answer to that is build much, much better information fields feeds elsewhere. Grins. Looks at me. No, no, you you do have to worry about it. But it's a different answer. It's a different answer.

00:32:55

That was nice.

00:33:03 Speaker 4

So I don't have to worry about it is.

00:33:05 Speaker 4

What I'm is.

00:33:06 Speaker 4

It sounds like the answer.

00:33:07 Speaker 4

Is I don't have to worry about it.

00:33:12 Speaker 4

OK. I'll follow up more later when it.

00:33:13 Speaker 4

Comes up, yeah.

00:33:18 Speaker 2

Yeah, I mean the we are in an interesting environment, not normally. Most of this would be done by government, must it be quietly handled, it's it's unusual.

00:33:33 Speaker 2

My my background is in crisis response.

00:33:39 Speaker 2

And my background in the last 10 years has been in crisis response and.

00:33:45 Speaker 2

I am much more used to doing this kind of thing in countries where the governments collapsed.

00:33:52 Speaker 2

Are you know we are where we are?

00:33:56 Speaker 9

Well, I was going.

00:33:56 Speaker 2

Doing what we're doing.

00:33:56 Speaker 9

To I mean, I mentioned that early on.

00:33:59 Speaker 9

With the activation group was.

00:34:03 Speaker 9

Team security.

00:34:05 Speaker 9

You know, we should probably have.

00:34:08 Speaker 9

To [Name Redacted] point, right.

00:34:12 Speaker 9

Don't don't know.

00:34:15 Speaker 9

How we're going to become targets too.

00:34:18 Speaker 9

I mean, we already are.

00:34:22 Speaker 9

Not that that's a bad thing or, but I mean, it's probably something that should be considered in.

00:34:28 Speaker 9

I know certainly if you're doing any kind of.

00:34:33 Speaker 9

Certainly in hot zones part of your training is is is personal security and.

00:34:40 Speaker 2

Yeah, I mean.

00:34:41 Speaker 9

What you're doing, so it might be worth incorporate.

00:34:43 Speaker 9

Folding that in.

00:34:45 Speaker 2

We should talk about OPSEC anyway, given we've got one of the world experts hiding in this room.

00:34:51 Speaker 2

But really, generally, if we're we're doing tracking and tracing on on disinfo campaigns, we we were very, very careful about OPSEC last year.

00:35:01 Speaker 2

And the year before, by now, everybody and their dog is doing this.

00:35:06 Speaker 2

Now I think that one is well and truly out of the gate.

00:35:11 Speaker 3

Yeah, if if if, if need be getting.

00:35:18 Speaker 3

Security trainings for like off second per second stuff.

00:35:23 Speaker 3

That is.

00:35:25 Speaker 3

Like that's viable, but I do not want to waste time giving it to people who.

00:35:34 Speaker 3

Like I will not give it.

00:35:35 Speaker 9

Turn that turn. You need it.

00:35:37 Speaker 3

Yeah, I'm not going to give it to the disinformation channel. There's not 6.

00:35:40 Speaker 3

150.

00:35:41 Speaker 3

People that I'm.

00:35:42 Speaker 3

Going to waste my time giving free apps like trading on.

00:35:46 Speaker 2

I mean, when there were five of us in the world, it made sense now.

00:35:47 Speaker 3

If there's.

00:35:49 Speaker 2

There's, like hundreds. It's yeah.

00:35:53 Speaker 3

And then, yeah, when I was doing like.

00:35:56 Speaker 3

And as they.

00:35:56 Speaker 3

Encounter disinformation stuff in 16 I had to do it by recruiting.

00:36:05 Speaker 3

They recruited a.

00:36:07 Speaker 3

Person to and then I had to regulate them into doing everything for me under his name.

00:36:19 Speaker 3

Worked quite well for me, but now suddenly he's got quite a lot.

00:36:23 Speaker 3

Of credit for what he did.

00:36:25 Speaker 2

Yeah, I had the same problem.

00:36:30 Speaker 2

That's OK.

00:36:31 Speaker 3

So yeah, OK. But yeah, like security for, for people who are actually doing things fine.

00:36:45 Speaker 3

I'll be happy to.

00:36:46 Speaker 3

Address what I can with that.

00:36:51 Speaker 2

I mean, don't go wading into the middle of a Q and on discussion with your real name screaming. Hey, I'm here.

00:36:57 Speaker 2

There, there are some being sensible things.

00:36:58 Speaker 3

Yeah. Look like flat out if, if.

00:37:04 Speaker 3

Like, if you're going to be doing things or probably have to do some procedures of things to take for.

00:37:08 Speaker 3

Security precautions like.

00:37:13 Speaker 3

Like one thing we're going to.

00:37:14 Speaker 3

Have to do is you might.

00:37:17 Speaker 3

Seriously, get people thinking about setting up a compartmental persona that they use all the time for their investigation. Because when they get boxed, which?

00:37:33 Speaker 3

It's like it's not inevitable, but it's a serious risk.

00:37:39 Speaker 3

You want the person that gets boxed boxed to be a nonexistent person, and you know, like there's a lot of people who.

00:37:51 Speaker 3

You know, they decide that they'll use like tool browser while they do their stuff and that will be sufficient.

00:38:00 Speaker 3

Or if they use, you know like.

00:38:06 Speaker 3

Incognito mode or some other very minor thing that they don't think about all the stuff like.

00:38:11 Speaker 3

You know their phone number that they've got Facebook cookies all over the place.

00:38:18 Speaker 3

That, you know, like they they don't have a dedicated e-mail which is useful to this, that that all these other things.

00:38:25 Speaker 3

And together.

00:38:26 Speaker 2

You gotta assume that if people have made it to this channel, they've they're, they've got some level of security.

00:38:36 Speaker 3

We can just formalize the very.

00:38:36 Speaker 2

Don't forget I said that.

00:38:37 Speaker 3

Basics and make sure everyone's on.

00:38:39 Speaker 3

The same? No, no, it's just.

00:38:41 Speaker 3

Like it's make sure everyone's on, you know.

00:38:45 Speaker 3

At least on ******* level 0, so.

00:38:49 Speaker 3

We're good. I nominate someone else to like that because apparently we're all at the level where someone.

00:38:56 Speaker 3

We should know the basics so.

00:39:00 Speaker 2

OK. We'll put that in the big book.

00:39:01 Speaker 3

OK.

00:39:03 Speaker 10

I'm happy to write up my basics. I am nowhere near as good as you guys, but I I'm happy to write it up as.

00:39:09 Speaker 10

Like the the.

00:39:10 Speaker 9

Yeah, I was just suggesting it more.

00:39:11 Speaker 2

Blessing. Yeah.

00:39:12 Speaker 2

Can you put it in the big book?

00:39:15 Speaker 10

Yeah, absolutely. I've I've. I've been going through it the last couple of years trying to do it myself. As someone who's never been into this kind of stuff before, and I've just been an educator, a teacher and now a tech director. And so I've had to think about this stuff in new and different ways. So yeah, I'm happy to write it up as just like the.

00:39:32 Speaker 10

The person going through the process and then you.

00:39:34 Speaker 10

Guys, absolutely. I would love people to add.

00:39:36 Speaker 10

All of their expertise to that.

00:39:38 Speaker 2

Sweet. I mean, if you put a section of the big book on it, then yeah, we can.

00:39:42 Speaker 2

Just kind of look at.

00:39:42 Speaker 2

It and and I can test it, I can be your test not done before it. OK, right. We've done tactical execution level.

00:39:53 Speaker 2

So the things we actually do inside CTI, so we're in CTI, which means we can spot disinformation instance and we're also connected to COVID-19 activation which is.

00:40:08 Speaker 2

A team we.

00:40:08 Speaker 2

We're talking to this morning and COVID-19 disinformation.

00:40:13 Speaker 2

So they come up with disinformation information. Cti comes in with it. Cti, other other teams bring us stuff.

00:40:20 Speaker 2

Sometimes. So we we get fresh fresh meat.

00:40:24 Speaker 2

At a point where we can actually still do something as a response rather than, this is like an interesting thing we can just investigate this.

00:40:32 Speaker 2

So get alerts, gather data.

00:40:36 Speaker 2

And the things we care about is, where did this come from? So track this thing back.

00:40:42 Speaker 2

See if we can stop it early.

00:40:44 Speaker 2

Understand how this is happening. Understand mechanics, because if you understand mechanics, you can then start understanding how to how to how to slow it down or stop it and find those weak points as part of that mechanics are there are there points at which you can you can divert the flows.

00:40:59 Speaker 2

I mean stupidly simple things like, you know you could camp on somebody's hashtag.

00:41:06 Speaker 2

Completely mess up the day. Stares at Greg and.

00:41:12 Speaker 2

A separate thing is analysis, so it's possible we're gonna have separated collection and analysis tasks.

00:41:19 Speaker 2

So you're looking for the date through the day you're looking for the trends in there?

00:41:23 Speaker 2

And you need.

00:41:26 Speaker 2

To produce enough information so some of this is about weight of evidence.

00:41:32 Speaker 2

Before you act, but also it's about getting enough information to an organization that can act. So you're saying to one of the registers. Please take this URL down.

00:41:42 Speaker 2

Don't just get enough information to say. Yeah, this person is selling MMS on this site. That's that's a nice simple.

00:41:49 Speaker 2

UM, you know, there's a crackdown on that. You can just post it straight over.

00:41:55 Speaker 2

Some of them might be more subtle, so get enough information that they can. They can take action, get enough information so that we know which counters to take, or the other thing is that.

00:42:09 Speaker 2

As we collect, we've got toolings and connect automatically back to previous events. So we can start connecting across and not not just to.

00:42:20 Speaker 2

Previous events that we've had we've seen.

00:42:23 Speaker 2

Like pandemic, we've actually seen pandemic sitting in an event back at the beginning of April, we just didn't notice we we didn't see it there.

00:42:34 Speaker 2

And across to the other teams. And then countering mitigation and then learning because like learning loops so execution loops.

00:42:44 Speaker 2

OK, which all gets us to.

00:42:47 Speaker 2

That's that's what we've been doing. So this is actually the thing we've been you've been seeing whilst we've been doing all this tactical stuff in the background, whilst above that, there's been all this operational strategic stuff going on.

00:43:01 Speaker 2

And it's all looked like a bit like, oh, my God, we're just running as fast as we can.

00:43:08 Speaker 2

And this gets us to this 500 people in one channel question.

00:43:12 Speaker 2

So we've got 500 people sitting in the disinformation channel.

00:43:19 Speaker 2

Out of that, we've got about 20 people who are really active in there.

00:43:24 Speaker 2

And we see you.

00:43:26 Speaker 2

We see you coming to the meetings. We we see you turning up on the channel. We see you when we say.

00:43:31 Speaker 2

Can someone help?

00:43:33 Speaker 2

So how do we make that work better?

00:43:38 Speaker 2

Both in.

00:43:41 Speaker 2

How do we make the flow of work better?

00:43:47 Speaker 2

So when you come in, you can see what needs doing. We can see who needs what, how it's going together, skill tree.

00:43:55 Speaker 2

[Name Redacted], was that you?
00:43:59 Speaker 2

Skill tree what's the skill tree?

00:44:02 Speaker 5

Ohh, like in a in a video game when you level up your character you.

00:44:05 Speaker 5

Unlock new skills.

00:44:07 Speaker 5

I just have to bring some [Name Redacted].

00:44:08 Speaker 5

Style to the to the.

00:44:09 Speaker 2

Room, you know. Yeah, OK, we've got video games.

00:44:18 Speaker 2

So yeah, I mean it's, it's his idea all. We're all learning together. We're building this thing together, but we're learning together as well. So one of the things is instant managers.

00:44:28 Speaker 2

Am just adding incidents and I seem to end up running all the incidents and checking in on all the incidents and it's just like I can't do 20 incidents.

00:44:38 Speaker 2

I I I've been sat trying to close them all down. It's just taking work.

00:44:43 Speaker 2

So the original idea was that.

00:44:47 Speaker 2

Somebody took responsibility for each incident and doesn't mean they.

00:44:50 Speaker 2

Have to have all the.

00:44:50 Speaker 2

Skills to run the incident.

00:44:53 Speaker 2

They're just responsible for finding the people that can actually do it do through the thing, but that needs a level of skill just to know how to look for them.

00:45:02 Speaker 10

So is that something that you could train?

00:45:07 Speaker 2

Yes, that's what we're talking about, the skill tree.

00:45:09 Speaker 2

So this is about us talking about what the roles across the team are.

00:45:14 Speaker 2

What we think as a team, they, they, they're they're going to be.

00:45:18 Speaker 2

And listing that out, training that up, it's getting a little bit more formal about the people part of this.

00:45:27 Speaker 2

Standing again at [Name Redacted]. Sorry [Name Redacted].

00:45:32 Speaker 2

The other people person, yes.

00:45:34 Speaker 7

Yes, ma'am.

00:45:37 Speaker 2

You understand the peoples.

00:45:37 Speaker 3

UM.

00:45:40 Speaker 7

You know, I understand the people, I I apologize. Help me understand the context context.

00:45:46 Speaker 7

Of your ask.

00:45:49 Speaker 7

You were talking about managing the incidents.

00:45:52 Speaker 2

OK. So what we're talking about is up to now, I've been just trying to manage about 20 instants at once, and it doesn't work right. So what we're doing is working out how to get other people, and there's a skill.

00:46:01 Speaker 7

Got it.

00:46:06 Speaker 2

To even if you can't do all the pieces, just managing getting the covered.

00:46:12 Speaker 2

So it's about listing out what it the instant manager does, how they do it, how they get the help, and just training people up. So this is all the skills leveling up, levelling up parts so.

00:46:27 Speaker 7

You have 20 active people. Of those 20 people.

00:46:33 Speaker 7

Because what I.

00:46:34 Speaker 7

See on the on the kind of the front end is I see, you know [Name Redacted] [Name Redacted], you know doing a lot of the kind of the back end build pieces, that's what I see. And and then I see you with the you know the incident part.

00:46:54 Speaker 7

What are the other so that that accounts for three the other 17? Who who are those in other individuals and what are the skills that they're doing?

00:47:06 Speaker 2

So [Name Redacted] has taken up a lot of the documentation site.

00:47:12 Speaker 7

OK.

00:47:13 Speaker 2

[Name Redacted] got laid off for a while because he he was doing his PhD, but he's back.
00:47:19 Speaker 2

So, [Name Redacted], what do you want?

00:47:21 Speaker 2

To be doing.

00:47:24 Speaker 1

Backing you up with whatever you need.

00:47:27 Speaker 2

OK, So what I've got down the bottom here is the list of things can. Can you see this list?

00:47:34 Speaker 2

Or do I need to make it?

00:47:35 Speaker 2

Bigger I'll make it bigger.

00:47:40 Speaker 2

So these are.

00:47:41 Speaker 2

All the things we've actually been doing.

00:47:45 Speaker 2

And This is why I don't sleep very much same.

00:47:51 Speaker 2

So that alert, collect, analyze, mitigate, loop the tech built.

00:47:56 Speaker 2

So we've been building out the tech we need, but we've been testing and documenting that tech. We've been designing the processes around this again, test and document.

00:48:04 Speaker 2

The big books.

00:48:06 Speaker 2

We are onboarding people, training people, buddying them up.

00:48:11 Speaker 2

So what you don't see is that every day I get at least half a dozen people will want to one chat with chat me.

00:48:20 Speaker 2

There's the log so that slide way up here where I just went sod it. I'm just not going to update this this time.

00:48:29 Speaker 2

It's like every three days I go back and work out what we'd be doing and just make sure we have a daily log and.

00:48:37 Speaker 2

Make sure we have a record of what we're doing. We're just that.

00:48:41 Speaker 2

That recording.

00:48:43 Speaker 2

Of what we do.

00:48:45 Speaker 2

So just that that's gripping.

00:48:48 Speaker 2

It is is.

00:48:49 Speaker 2

A is a thing in itself that that team tracking the team coordination across.

00:48:54 Speaker 2

Making sure it's all working as a team.

00:48:58 Speaker 2

The instant management itself, so individual instance from.

00:49:03 Speaker 2

Starting them, getting the data collection going, making sure that we've got all of the tool.

00:49:08 Speaker 2

Sets up through to populating those tools with the data through to working out which actions.

00:49:15 Speaker 2

So that I guess that goes back up to the look collection.

00:49:21 Speaker 2

That goes under there.

00:49:24 Speaker 2

But you can kind of see.

00:49:27 Speaker 2

All the pieces that have been happening in here and then clean up comes under there too, because.

00:49:34 Speaker 2

When we finish an incident, there's also the now we now we make sure it's written up, make sure the all the artifacts are hiding in the right systems.

00:49:41 Speaker 2

Ready for ready for next time, but there's also the Cross Instant management.

00:49:47 Speaker 2

So it's that and I ran a training on this.

00:49:51 Speaker 2

Couple of weeks ago.

00:49:53 Speaker 2

Which is the if we have multiple instances running, we have to decide which ones we actually prioritize, which ones we actually put team on because we know we don't have that much team yet.

00:50:06 Speaker 2

Some of this is like trying to make things simple enough so that people have single tasks. Some of this is like trying to make sure that.

00:50:13 Speaker 2

That all the people who have specialist skills have work that is comfortable for them. So you you have people like [Name Redacted] who is doing a very specialized piece of research.

00:50:27 Speaker 2

Quietly off to one side because she's a data scientist who can do that very, very, very involved.

00:50:38 Speaker 2

And we have different people who will work better in teams.

00:50:43 Speaker 2

So it's a girl that I didn't even put. Team management suck. Yeah, my.

00:50:49 Speaker 7

That's kind of where my head was going as. So I'm kind of seeing a couple of things here because like you said, we're, you're we're all building the plane while we're flying in it.

00:50:58 Speaker 7

And unfortunately, the passengers kind of freak out when.

00:51:01 Speaker 7

You ask them to hold the.

00:51:02 Speaker 7

Tools for you, right? Yeah.

00:51:04 Speaker 7

So, well, you know, in my experience, they scream a little. So I'm kind of hearing a couple of things. I'm I'm hearing that you need good incident managers and you need.

00:51:18 Speaker 7

You know the scribes. Like you said, you definitely.

00:51:21 Speaker 7

Got the tech?

00:51:22 Speaker 7

I haven't seen the level of talent.

00:51:25 Speaker 7

Anywhere else in the league then then this team here, which is kind of cool.

00:51:32 Speaker 7

Also sorry for my cat.

00:51:32 Speaker 2

Nice guys. Bye bye.

00:51:36 Speaker 2

The cat's just agreeing on the tech.

00:51:38 Speaker 7

Yeah, he is. He's like, right. So the other piece that I was going to say is like the OPSEC pieces of it, like.

00:51:46 Speaker 7

That the [Name Redacted] cat is just old.

00:51:52 Speaker 7

So the other piece is like there's who, like the people that maybe report the information, like which one of us has, you know, the good sock puppets that can hide behind the VPN's and you know, use, you know, the the voice over IP phones.

00:52:12 Speaker 7

That that sort of piece, right that was.

00:52:13 Speaker 7

Being referenced earlier.

00:52:17 Speaker 7

That that. You know what, what are those needs? Can we break it down that simplistically?

00:52:23 Speaker 7

And see whether can those talents split.

00:52:23 Speaker 9

Well, and do we need to?

00:52:24 Speaker 9

Do that actual.

00:52:26 Speaker 9

And do we need to actually do that work too? Because we also have this activation network of a bunch of actual people who we can feed this the counter information and they can they can pump out the the the counter information without having to you know if if we set them up for it.

00:52:35 Speaker 2

Requested, yeah.

00:52:38 Speaker 7

Right.

00:52:46 Speaker 9

Because they're also a listening additional listening post too.

00:52:47 Speaker 2

Yeah, I mean.

00:52:50 Speaker 2

So we've got the slack pillars. We've got a second myth. So the COVID-19 activation, COVID-19 disinfo teams can.

00:52:51 Speaker 7

That's fair.

00:53:02 Speaker 2

Use the same tool link. Poke into a second mist that we link across to our mist so we're air gapped.

00:53:09 Speaker 2

So we could do that too, so they don't even need to be.

00:53:12 Speaker 2

Inside this team.

00:53:14 Speaker 2

We can just put request for.

00:53:15 Speaker 10

And [Name Redacted].

00:53:15 Speaker 9

Information. It's always, I mean that's that's been one of the design thoughts, right is that we would allow things to perk, pull up, up and go in all those directions. And that's why those silos are there, right.

00:53:16

Well that.

00:53:26 Speaker 10

Yeah. And I think to Jr's point, though, we we do need to have some OPSEC pieces around helping people just lurk in the places to find the information to understand what's going on, to then feed to the people who take the active measures.

00:53:38 Speaker 2

Yeah, yeah. I mean like when the Q and on call went out the other day, I would have loved to have had a sock puppet just respond to that so they could get the command.

00:53:45 Speaker 2

Command calls.

00:53:47 Speaker 9

Yeah, I mean sending it to the slack channel on on, on COVID activation, you know then then you've got a group of 500 people over there who monitor that Channel who can pick up things and.

00:53:58 Speaker 7

Well, like [Name Redacted] does, [Name Redacted], you know.

00:54:02 Speaker 7

Cause sort of those.

00:54:03 Speaker 7

Early days when I was chasing some of that Q and on.

00:54:07 Speaker 7

Fees that were going to that mobile app and then I I, you know, found those onion sites and I I have like a solid sock puppet right now on Twitter. All I did was follow a couple accounts and then the rest of them all just flood.

00:54:23 Speaker 7

Then, so you know, there's some of us that are decent enough that if we're getting enough of the.

00:54:30 Speaker 7

Tip we can poke like like a couple others just.

00:54:32 Speaker 7

Said that, if there's something actionable, we can at least poke.

00:54:35 Speaker 7

Enough comfortably to say there's there might be something here that might not be or whatever to make sure that our time is worth it.

00:54:44 Speaker 2

But some some of this is just like working out which skills we have across the team and then working out how we match that across. The other thing is is building just structuring the team across this.

00:54:48 Speaker 7

Right.

00:54:56 Speaker 2

So it's just working out how to how.

00:54:57 Speaker 7

That's correct. And that's my point.

00:54:58 Speaker 2

To put this together.

00:55:01 Speaker 7

Yes. Yeah. So do you do you need scribes? Do you need? You know, how many incident managers do you need that can just focus on?

00:55:12 Speaker 7

You know, just closing out those cases. Do you need a, you know, a couple of offsets? Do you need back end folks like those are the, I guess those kind of where I'm looking at it.

00:55:25 Speaker 7

Am I on track? Yeah.

00:55:26 Speaker 2

Folks, you're on track.

00:55:27 Speaker 7

Yeah, I'm turning to the rest of the group.

00:55:32 Speaker 5

Yeah, this was. This was basically the conversation that [Name Redacted] and and [Name Redacted] myself just had. And those are very much roles that we need to identify and and start casting people into. I think as just as just getting at you know part of it is identifying what those rules are but also identifying who who we have as a resource that we can put in those roles. So there's a.

00:55:52 Speaker 5

Bit of a chicken and egg thing there. I think you know that boils down to community management. When we first need to just see who do we have, what can we do with with.

00:56:03 Speaker 5

The folks we have so.

00:56:06 Speaker 2

But I also wanted to do this as a team. I didn't want to just like turn up and go guys. We're just gonna change everything on.

00:56:11 Speaker 2

You and by the way, you over there. You just became an instant manager.

00:56:16 Speaker 2

It's like this has to be the team puts this together.

00:56:20 Speaker 6

I am a leaf on the wind. Watch me float.

00:56:26 Speaker 7

Do they get cool sashes? That's.

00:56:26

I I.

00:56:28 Speaker 7

All I want to know.

00:56:30 Speaker 2

What's like a cool sash? We're going to rain sashes.

00:56:34

I don't know.

00:56:34 Speaker 6

About sash but I am getting some custom made face masks done.

00:56:40

That's good.

00:56:40 Speaker 6

That has the CTI logo across the front of them.

00:56:44

Stop it.

00:56:44 Speaker 2

OK.

00:56:47 Speaker 2

We all right? All right. We should have swag, OK?

00:56:51 Speaker 6

I I made it for myself, but if y'all would like one, I can definitely just give you the URL and.

00:56:56 Speaker 6

You can order one up.

00:56:58 Speaker 2

Yeah, I mean.

00:56:58 Speaker 6

Schwag kind of person I like. I grew up on Schwag.

00:57:01 Speaker 1

Yes, please.

00:57:03 Speaker 2

Yeah, I mean you.

00:57:04 Speaker 2

Know you, you do. You take the responsibility, you get the swag. It's.

00:57:07 Speaker 2

Gotta be done.

00:57:09 Speaker 6

It doesn't say anything about our team, it just it's just a generic CTI logo.

00:57:15 Speaker 2

We can adapt it.

00:57:17 Speaker 6

Oh yes.

00:57:18 Speaker 2

But OK, yeah. So we're we're going to.

00:57:20 Speaker 2

Each. So we basically need to list out the skills and work out who is prepared to do this and timings. I mean the other thing is work out who is available when.

00:57:31 Speaker 2

UMI don't think we can run a 24/7 operation.

00:57:36 Speaker 2

But luckily the bad guys aren't able to.

00:57:36 Speaker 3

Speaking of available when?

00:57:39 Speaker 6

Well, now I'm available more, so don't be. Don't be disappointed if I end up doing things at 3:00 in the morning.

00:57:40 Speaker 3

I I'm off.

00:57:46 Speaker 2

Not disappointed at all. I'll see you there.

00:57:55 Speaker 2

So basically just working out roles, role lists, skills, just how we get there from here.

00:58:03 Speaker 2

And keep with the building out the process and toolings and making this work.

00:58:12 Speaker 2

Does this seem like a reasonable plan?

00:58:22 Speaker 6

I say yes.

00:58:25 Speaker 2

OK.

00:58:26 Speaker 8

I'd be happy to take up, you know, few incidents once you know, once I get into, you know, I I once I get a grasp of of everything also in a different time zone. So it might be an advantage.

00:58:46 Speaker 2

That that helps. I mean, we wrote, wrote the reading of the big book to to make it easier. So I guess we just keep doing.

00:58:55 Speaker 2

I I guess we can write out roles and stuff in the big book.

00:58:58 Speaker 2

I would still work.

00:59:02 Speaker 2

I know I love.

00:59:02 Speaker 2

The big book.

00:59:05 Speaker 7

I'm a fan of big books.

00:59:08 Speaker 2

Yeah, well, it just makes it easier to have one place to go find everything.

00:59:11 Speaker 6

I like big books and I cannot lie.

00:59:15 Speaker 2

I was waiting for that.

00:59:20 Speaker 6

Well, I'm glad it isn't. For once, I didn't disappoint. So there you go.

00:59:20 Speaker 7

You win Wednesday.

00:59:25 Speaker 2

Thank you, Sir. [Name Redacted] a lot.

00:59:30 Speaker 7

I I totally got you for team betting.

00:59:35 Speaker 7

If you like you.

00:59:38 Speaker 7

You definitely can count me in on that.

00:59:41 Speaker 7

And and then if you want me to run any osment on anything.

00:59:48 Speaker 7

You can count me on.

00:59:49 Speaker 7

That for sure.

00:59:50 Speaker 2

Cool. And and we can just start with the the new channel bring people, just pull people in and just get ourselves started and pointing in the right direction.

01:00:02 Speaker 2

Because that was the other thing that was worrying was just like doing all of this with 500 unknown people watching.

01:00:09 Speaker 2

It's kind of nice because you get to show 500 people what you're up to.

01:00:12 Speaker 2

But it's also the.

01:00:20 Speaker 7

Literally, [Name Redacted] and I were just talking about that last night, so.

01:00:28 Speaker 2

OK, I think we managed to run over the top of the training time.

01:00:33 Speaker 9

No, we're just about, we just hit it.

01:00:35 Speaker 9

It's just 5:00.

01:00:37 Speaker 2

Yeah, we were gonna train up on Amit's tactics techniques, procedures, but OK. So I guess we'll do that next time.

01:00:46 Speaker 2

Unless anyone wants to spend another half hour. Otherwise, comments, thoughts. Any other things we need?

01:00:53 Speaker 6

The automated search system is now completely automated and running on its own.

01:00:59 Speaker 6

So the.

01:01:01 Speaker 6

If you go into our other Slack channel, you'll see just about every 30 minutes. It will update with any hashtags and seen both in the direct and the matrix search that have registered more than fifty hits.

01:01:15 Speaker 6

Nice. And that's been running overnight, completely automated by itself, and it's been happy. So I'm happy and I fixed the problem with the counting the database. It was a silly mistake on my part and I fixed it and I went back and I think I fixed everything. So we have at least 898%.

01:01:38 Speaker 6

The only thing that that 2% is just my paranoia talking.

01:01:38

OK.

01:01:42 Speaker 9

Is this this disinformation managers channel that you're talking about?

01:01:46 Speaker 6

No, there's a slack channel. It's called disinformation fee. What is it? Twitter disinformation streaming.

01:01:55 Speaker 9

In CTI.

01:01:57 Speaker 6

Yes, it's under the number 3 heading.

01:01:58 Speaker 5

OK. Yeah.

01:02:00 Speaker 6

It's two above us. We're #4 disinformation.

01:02:04

I don't.

01:02:04 Speaker 6

And above us is dark net. And then there's #3 Twitter disinformation.

01:02:08 Speaker 2

This information is streaming.

01:02:10 Speaker 2

I guess start now.

01:02:10 Speaker 9

Yeah, I don't see it some reason.

01:02:13 Speaker 6

Hmm, you may. You may need to be invited to it.

01:02:17 Speaker 8

Yeah, I don't see it either.

01:02:21 Speaker 2

I don't think it's.

01:02:23 Speaker 2

It doesn't look like a lock channel.

01:02:25 Speaker 6

You know what it is? It is. You have to be invited to it. I'm sorry. I didn't realize that when they created it.

01:02:31 Speaker 2

Well, I guess we'll just have to invite to that as well as.

01:02:33 Speaker 2

The other channel like I.

01:02:34 Speaker 6

No. Who needs to be?

01:02:35 Speaker 9

Invited unless did they mean to?

01:02:36 Speaker 1

Don't think I don't think it's.

01:02:37 Speaker 10

Locked. I just found it and got in. I think it's just not promoted on.

01:02:41 Speaker 10

The side.

01:02:41 Speaker 10

So if you have the.

01:02:41 Speaker 9

It's not on the. Yeah, OK.

01:02:44 Speaker 6

OK, I just started inviting people.

01:02:50 Speaker 2

OK so.

01:02:52 Speaker 6

Now there's more info than this to be had, but right now I'm trying to rig up a way for us to easily access it.

01:03:04 Speaker 6

Is everyone here familiar with SQL desktop?

01:03:11 Speaker 2

Kind of sorta.

01:03:13 Speaker 6

I'm seeing that's the way I want that that may be the way to go, but everyone have read only access to the database using SQL Desktop.

01:03:22 Speaker 4

So when you say SQL desktop or you're just talking about a desktop client app for accessing a SQL Server.

01:03:34 Speaker 4

OK. Yeah, because there are a.

01:03:36 Speaker 4

Lot of different.

01:03:37 Speaker 4

Versions of that just. I'll basically do the same thing.

01:03:38 Speaker 6

Yeah, there's a lot of different front ends too. That's just a. It's a nice graphical one and it it doesn't hurt very much. It's a lot less painful than directly logging in through a through a terminal.

01:03:49 Speaker 6

Which is, I don't know. Are anybody here familiar with this or has anyone not seen it before?

01:03:54 Speaker 4

I'm familiar with other brands that.

01:03:56 Speaker 6

Do something like.

01:03:56 Speaker 2

I've stopped share. You can share if.

01:03:58 Speaker 2

You want.

01:04:00 Speaker 6

Look, go ahead. You can share cause I don't have it up right at.

01:04:02 Speaker 6

The moment I'm trying to do something else.

01:04:03 Speaker 2

I don't have it up either so.

01:04:06 Speaker 6

Oh, someone just had it up a second ago.

01:04:07 Speaker 2

What everyone does but.

01:04:11 Speaker 2

Oh, I had the minions up. I had to.

01:04:12 Speaker 2

Treated information screen.

01:04:13 Speaker 6

Yeah, that's what I was talking about.

01:04:16 Speaker 2

Ohh that that was me so I'll share them again.

01:04:20 Speaker 4

Visualizer is the one that I was.

01:04:22 Speaker 4

Using OK SQL, SQL Workbench.

01:04:27 Speaker 6

Worked, but that's what I was doing. I'm sorry, SQL Workbench is what I'm trying to think of. So anyway, here's what this is for. Anyone who isn't familiar with it, there are two databases we're running right now. One is called the Matrix database and one is the direct database.

01:04:27 Speaker 4

Sequel pro.

01:04:29 Speaker 2

There you go.

01:04:42 Speaker 6

And the matrix.