Audio file

2020-07-01_Training_TheHive_[Name redacted].m4a

Transcript

00:00:12 Speaker 1

You look familiar.

00:00:14 Speaker 1

You all look familiar.

00:00:16 Speaker 2

I know.

00:00:35 Speaker 2

So [Name redacted], did they make you stop working from the office or are you still forced to work from the office and?

00:00:40 Speaker 2

You're just at home today.

00:00:44 Speaker 3

It is 7:00.

00:00:45 Speaker 3

Where I am so yeah, I had.

00:00:46 Speaker 3

To go into the office.

00:00:48 Speaker 2

That is the stupidest thing.

00:00:50 Speaker 2

I have ever heard. I'm so sorry.

00:00:53 Speaker 3

Yeah. Thanks. It's, it's ridiculous. I yelled at HR today. So at least that happened.

00:01:04 Speaker 3

The result of that conversation was her saying. Well, do you think we?

00:01:07 Speaker 3

Can ever come?

00:01:07 Speaker 3

Back and I was like, well, when you guys provide sufficient PPE and there's a vaccine that would be great.

00:01:16

Thank you.

00:01:17 Speaker 3

I'll laugh. I'll be there again tomorrow. What's that?

00:01:21 Speaker 2

I have a friend who worked in New York and he was like we should start getting people to come back to the office and he's like, well, are you going to start paying me hazard pay?

00:01:28 Speaker 2

Well, no. Then ****.

00:01:30 Speaker 2

Off I'll continue to work from home.

00:01:34 Speaker 2

[Name redacted], he's the director of it for that organization. So he has a little bit of clout in that regard, but.

00:01:42 Speaker 3

I'm the director of it for mine.

00:01:44 Speaker 1

If anybody should know if they have to go in, it should be the director of IT. If he can't dial in all of a.

00:01:48 Speaker 1

Sudden he knows he should go in.

00:01:50 Speaker 2

Spam right. Bam. Ohh.

00:01:53 Speaker 2

They were.

00:01:55 Speaker 2

We should we want to start going back into the offices.

00:01:58 Speaker 2

And he's like over my dead body.

00:02:00 Speaker 2

The only time out, the only reason I'm going into the office.

00:02:02 Speaker 2

Is if a.

00:02:03 Speaker 2

Machine actually, physically you know, starts to lose.

00:02:05 Speaker 2

A drive and then I will.

00:02:06 Speaker 2

Go in long enough.

00:02:08 Speaker 2

To to swap out a drive and rebuild the.

00:02:11 Speaker 2

Raid and then leave.

00:02:14 Speaker 2

Other than that, no.

00:02:17 Speaker 3

[Name redacted], can you check questions?

00:02:17 Speaker 4

We went to a completely new month.

00:02:31 Speaker 3

[Name redacted], can you check the questions on slide three to make sure that I ask the right questions.

00:02:42 Speaker 3

I'm shouting into the void, aren't I?

00:02:46 Speaker 2

No, I can hear you just fine. Don't.

00:02:48 Speaker 2

Think he cares, though.

00:03:12 Speaker 5

I guess I should share my screen.

00:03:19 Speaker 2

That's a neat new feature of zoom. They have an option for automatically copy the invite link to the clipboard once the meeting starts.

00:03:27 Speaker 2

Like they know.

00:04:11 Speaker 3

Is everyone else able?

00:04:12 Speaker 3

To work remotely, AM I the only?

00:04:13 Speaker 3

Person that has to go back to work.

00:04:15 Speaker 2

I mean, I've worked remotely for the past five years.

00:04:18 Speaker 2

Before that, it was like 3-2.

00:04:20 Speaker 4

What's an office?

00:04:24 Speaker 6

And luckily I don't. Nobody's forcing us to go back to work, so.

00:04:30 Speaker 6

Or go back to the office. I should.

00:04:31 Speaker 6

Say, still working? Yeah.

00:04:37 Speaker 5

It's optional for us.

00:04:40 Speaker 5

But so I'm going to.

00:04:41 Speaker 5

Stay home.

00:04:48 Speaker 3

I think I got to get myself.

00:04:48 Speaker 3

A job where I can work remotely after this.

00:04:56 Speaker 4

It has plus and minus, but I'm guessing.

00:04:59 Speaker 4

A lot of the.

00:05:00 Speaker 4

Things that used to be minuses get better after everybody does it for a year.

00:05:11 Speaker 6

Yeah, I'll say I think my team at work has gotten a lot.

00:05:14 Speaker 6

Better at collaborating remotely.

00:05:18 Speaker 4

Yeah, I mean, for a while it was just like you were the remote person and everyone ignored you.

00:05:25

Yeah, everybody's like.

00:05:26 Speaker 6

Five people in A room.

00:05:27 Speaker 6

With a whiteboard and one person on a video call. They can't really join in, it's.

00:05:35 Speaker 4

And they were just like the things that nobody ever thought about, like they'd go off and chat over coffee.

00:05:42 Speaker 4

And forgot to forget to include you or they forget to bring you back in after they came.

00:05:46 Speaker 4

Back from coffee or?

00:05:50 Speaker 4

Be waving at the screen.

00:05:58 Speaker 5

One thing I'm noticing and that I actually like, is they're far fewer meetings, or at least they tend to be more.

00:06:04 Speaker 5

Succinct, you know.

00:06:09 Speaker 5

When whenever we get on zoom typically like there's an agenda plot through it and not so much like, you know, time wasting. Yeah. So that's interesting.

00:06:20 Speaker 4

I pioneered 15 minute meetings when I was at.

00:06:25 Speaker 4

So we had if we had something to do, we we put the agenda up beforehand, wrote wrote. Our stuff in beforehand, the meeting was just like, ratify stuff.

00:06:33 Speaker 4

30 minutes. If it was more complicated.

00:06:39 Speaker 4

Because just in terms of the amount of time, OK, I'll stop taking up time.

00:06:44 Speaker 3

Now this is great. Cool. So maybe we'll give.

00:06:46 Speaker 4

People one more.

00:06:46 Speaker 3

Minute to come in and then I can.

00:06:48 Speaker 3

Get started.

00:06:50 Speaker 3

Welcome, [Name redacted]. Welcome [Name redacted].

00:06:54 Speaker 4

I put what's happened in this past week. Ohh hey.

00:06:59 Speaker 4

So I put what's happened in the past week into the team log in top of the Google Drive.

00:07:05 Speaker 4

Just so you can see what will be up to base, TLDR is minimum masks, March, there's new incident.

00:07:11 Speaker 4

We closed down some old institute incidents and we're talking about how to get these out to more responders.

00:07:20 Speaker 4

Parlay API clients gone in and.

00:07:27 Speaker 4

Documentation. We've got some more cool stuff in there.

00:07:30 Speaker 4

And hackathon Hackathon's coming up on us. So we've got two weeks to go till the all teams hackathon.

00:07:38 Speaker 4

So any ideas for that very, very welcome?

00:07:41 Speaker 4

OK, I've got my bed. You'll turn.

00:07:44 Speaker 3

Sweet. Cool. So, [Name redacted], can you?

00:07:48 Speaker 3

Go to slide 2 for me.

00:07:52 Speaker 3

Thank you, Sir.

00:07:54 Speaker 3

Cool. So today we're going to be diving into the hive and incident management and we're going to try to use a framework that I've used in a bunch of other kind of professional learning settings before. And if it completely fails, I'll blame it on myself. It's called the dilemma consultancy protocol. Basically, the idea is.

00:08:13 Speaker 3

We have a framing question. Then we're going to have an introduction. [Name redacted]'s gonna present the dilemma, including just like the overall what the hive is. And then frame that question for us. Then we get a few minutes for clarifying questions. Few minutes we're deeper probing questions and then open discussion and then [Name redacted] kind of responds with what?

00:08:32 Speaker 3

Was useful to him.

00:08:33 Speaker 3

And then we debrief the process.

00:08:35 Speaker 3

And we go from there.

00:08:38 Speaker 3

That's basically the flow any.

00:08:40 Speaker 3

Questions about the general process.

00:08:50 Speaker 3

Awesome. Cool. So, [Name redacted], with that, I will let you take it away.

00:08:59 Speaker 5

OK, thanks. So our framing question, I think this thing we're really trying to answer here is, is the hive the correct tool for incident management. We we want to identify what's working, what is int.

00:09:17 Speaker 5

And next steps that can.

00:09:20 Speaker 5

More useful or better fit what we're.

00:09:22 Speaker 5

Trying to do.

00:09:24 Speaker 5

The reason this is an important question or it's going to drive a lot of the case management talk today, is that the hive is really meant to speed up incident response. It's supposed to be a platform that makes analysis quicker.

00:09:40 Speaker 5

And so if it's failing in that capacity, if we're not actually improving our response time, if we're not making our.

00:09:46 Speaker 5

Lives easier and we're bottlenecked by the by the technology. Then it's failed in its goal and we need to reevaluate what we're using or what we're trying to do.

00:09:59 Speaker 5

So disinformation incidents.

00:10:05 Speaker 5

Are interesting. They're composed of time.

00:10:10 Speaker 5

Resources, infrastructure, execution requirements or restraints, and there are multidisciplinary so we have infosec, data, science, social sciences, all of these domains coming together to to build these incidents for campaigns. That means when we respond to them.

00:10:31 Speaker 5

They're very complicated and we're not going to have one.

00:10:36 Speaker 5

Single pattern that that's appropriate for responding to all all incidents. Instead we have to find ways.

00:10:44 Speaker 5

To break that down and.

00:10:47 Speaker 5

What incident workflows can do is help us frame the the problem or the incident we're trying to work with, and our framing might be by application of and it's tactics or techniques, for example.

00:11:04 Speaker 5

A workflow might look at how personas are developed and how its informant is generating the accounts used in their campaign and and and walk through like the appropriate steps for that.

00:11:16 Speaker 5

And these workflows define the procedures within that frame. So like what are the steps we're looking at, what are the technical procedures, what are the investigation procedures we want to look at and so on.

00:11:28 Speaker 5

And finally, these workflows indicate our.

00:11:31 Speaker 5

Progress. So we need to be able to keep track of who's done what, how deep down the rabbit hole we are, whether or not something's been looked at.

00:11:43 Speaker 5

So workflows as they're actually implemented in the hive.

00:11:49 Speaker 5

Is is pretty simple. They're they're really just a set of tasks. It's a list of tasks and that's it. We're going to use them in the hive to we're how we're currently using them really is to define like, say in investigation steps or minimum investigation.

00:12:09 Speaker 5

That's arguably most importantly to to breakdown complex investigations into distributable chunks because we're operating as a distributed team.

00:12:21 Speaker 5

In a complex investigation, we just want to be able to like task out things to individuals.

00:12:25 Speaker 5

And not have not.

00:12:27 Speaker 5

Require them to know everything that's going on in the in the investigation.

00:12:31 Speaker 5

And also to provide guardrails just to kind of keep people on the right track.

00:12:38 Speaker 5

So I think everyone here has seen cases in the hive cases basically just like a title, some artifacts or observables, you know like IPS or whatever, some notes and a list of a list of tasks.

00:12:55 Speaker 5

For task log.

00:12:58 Speaker 5

And as we're working through tasks or these cases, everything gets updated in real time, so we'll have some visibility into if other people have completed something.

00:13:08 Speaker 5

That's like related to what we're working on.

00:13:16 Speaker 5

Case templates as we've used them so far, have have only been for the purpose of a base template. When we create a new disinformation incident we we start with our template.

00:13:27 Speaker 5

It says like, OK, this is a disinformation incident. Here's the TLP or the OR the PAP settings, minimum tags and go and create this miss event. Go create a decant folder. Tell people in the channel what you're.

00:13:41 Speaker 5

Working on so.

00:13:43 Speaker 5

It's basically just the skeleton to get things set up.

00:13:46 Speaker 5

But it does not inform us how to actually do any work.

00:13:49 Speaker 5

And that's what we're going to look at, that's.

00:13:52 Speaker 5

What we want to build.

00:13:54 Speaker 5

So these workflows what they actually look like.

00:14:01 Speaker 5

These are the tasks.

00:14:02 Speaker 5

And this is what I'm talking.

00:14:02 Speaker 5

About when it's a list of tasks.

00:14:05 Speaker 5

And these tasks can be grouped and here where it says collection this is a grouping.

00:14:14 Speaker 5

It's arbitrarily defined, so if we wanted to have, you know, like developed people or go physical and tactic grouping, that would make sense.

00:14:22 Speaker 5

If we prefer something like the incident response life cycle where you know we do like collection investigation remediation or whatever we could do that as well.

00:14:31 Speaker 5

So it's really up to us to decide how we want to frame those those groupings for what we're looking at.

00:14:39 Speaker 5

And because these are linear, we just step through them.

00:14:42 Speaker 5

For that reason, it's better to keep it simple. Shouldn't try and over engineer logic if we want to have like.

00:14:49 Speaker 5

You know, like conditionals. Like you know, if you do this task then go and create these new tasks. We're doing something wrong that's far too complicated.

00:14:59 Speaker 5

And slow. It's better to abstract that stuff out into a platform meant for handling, something like that.

00:15:11 Speaker 5

So an actual task. This is what it looks like when you create when.

00:15:16 Speaker 5

You create a new one.

00:15:18 Speaker 5

It's just the title.

00:15:19 Speaker 5

It's a group.

00:15:21 Speaker 5

And your description is the you know the text that describes what the task is that you have to complete. It's written in markdown.

00:15:30 Speaker 5

We can include images or like tables or links or whatever. That's fine, and then optionally assign it to an individual. So there might be some tasks where we require a domain expert or.

00:15:46 Speaker 5

An analyst to triage something and so that might be useful for us. Just something to.

00:15:53 Speaker 5

Keep in the back of your mind.

00:15:57 Speaker 5

And after we've created our task or our new case template.

00:16:01 Speaker 5

And we have to merge them into our current our current task that's open.

00:16:07 Speaker 5

So I'll go back to this view. Let's say we open here case 40, persistent anti VAX.

00:16:16 Speaker 5

And then we want to go and add a new workflow here. Like I don't know, go and investigate, you know, account creations or research the users avatar to check if it looks like it.

00:16:31 Speaker 5

A deep if it's a deep faker look, whatever the case is, we're going to merge that new case that we open the new workflow.

00:16:40 Speaker 5

Into the previous one.

00:16:43 Speaker 5

And there's one warts on on all of that when when we do this, it generates.

00:16:51 Speaker 5

A long ugly case name.

00:16:54 Speaker 5

We could remove that with some automation. A good idea for the hackathon we have coming up would be to actually add a feature to the hive that allows us to merge new case workflows without needing to create a secondary case, but that's like that's the side point.

00:17:14 Speaker 5

So that's really the gist of it. We just want to use these case templates to frame a problem, walk through the steps, and then merge these.

00:17:24 Speaker 5

These cases into whatever it is we're working on.

00:17:28 Speaker 5

And for.

00:17:30 Speaker 5

Next steps.

00:17:34 Speaker 5

As I mentioned.

00:17:35 Speaker 5

The the framing is important I think.

00:17:39 Speaker 5

Might actually be the most important thing when we're talking about the workflows, because we don't need to store all of the.

00:17:47 Speaker 5

High fidelity.

00:17:49 Speaker 5

Details of how to perform the task we have experts and we can refer to outside materials. You know, like the big book or or whatever, whatever else that really step by step walk.

00:17:58 Speaker 5

Through walk through it.

00:18:00 Speaker 5

But it's important to know like what the question is we're asking and and how we think about the problem. You know, do we want to?

00:18:06 Speaker 5

Do we want to approach an incident?

00:18:08 Speaker 5

As a tactic from Yammer framework, do we treat it more like?

00:18:12 Speaker 5

Incident response are there, you know, other things we might do like.

00:18:19

I don't know.

00:18:19 Speaker 5

Computing hypothesis is something interesting that [Name redacted], and actually we're telling me about the other day.

00:18:25 Speaker 5

That might fit in here.

00:18:28 Speaker 5

So that's yeah. So that's it, high level.

00:18:33 Speaker 5

This is how we're going to set up tasks and I'll hand it back to [Name redacted].

00:18:40 Speaker 3

Sure. [Name redacted], did you want to take a minute to just walk us through?

00:18:42 Speaker 3

The creation of that.

00:18:46 Speaker 3

Trusted source thing that you were talking about.

00:18:49 Speaker 3

When we chatted earlier or does that not fit quite what you were thinking?

00:18:54 Speaker 5

Creation of a trusted source.

00:18:57 Speaker 3

Well, you're gonna create like a new workflow for like is this a real person or is this A is this a real authority? I think maybe.

00:19:04 Speaker 5

Yeah. Let me show you that. So yeah. So take experts, I believe. So what?

00:19:11 Speaker 5

We talked about.

00:19:11 Speaker 3

Right, right. Experts. Yeah.

00:19:13 Speaker 5

OK, so I'll.

00:19:14 Speaker 5

Make this a little bigger so it's easier to see.

00:19:18 Speaker 5

If we want to add a new case.

00:19:22 Speaker 5

Workflow or it's really it's a case template, so here under admin.

00:19:28 Speaker 5

This is our.

00:19:28 Speaker 5

Case template management view we click new template.

00:19:35 Speaker 5

Assign it a name. So let's do.

00:19:40 Speaker 5

Sir, 9.

00:19:44 Speaker 5

These fake experts.

00:19:47 Speaker 5

Title prefix.

00:19:54 Speaker 5

And add a description so this workflow examines fake experts their credentials.

00:20:09 Speaker 5

So that's that's the case templates metadata that tells us what we're working with all of the magic happens over here under tasks.

00:20:18 Speaker 5

So you click there to add a task and add a a title. So like what is the job the group where does it belong and the description and so the title might be something like.

00:20:32 Speaker 5

Check publication. So this is a question for you, [Name redacted]. If somebody publishes a fake paper and they say it's cited and it's not, how would you look that up quickly?

00:20:44 Speaker 5

Is there like?

00:20:44 Speaker 5

A A database or.

00:20:46 Speaker 5

Something or or like a university.

00:20:49 Speaker 3

I thought, yeah, I tossed to [Name redacted].

00:20:51 Speaker 3

On that one.

00:20:54 Speaker 4

Sorry, what was the question?

00:20:56 Speaker 5

So if for fake experts, if somebody publishes like research or claims to have published research, how would you go and where would you verify that first like you would look it up in like a university library index? There must be some like database that compiles all of these sources together. Do you know what it's called?

00:21:14 Speaker 4

There are a bunch of academic paper places, so you can go check. So if they say they published it, you check the place they said they published it, see if they've got it listed. If they say the part of the university, you check the university site.

00:21:32 Speaker 4

And then you go and look at things like the pre publication sites and.

00:21:37 Speaker 4

The conference listings.

00:21:41 Speaker 4

But people don't generally publish just white papers. We do. Sometimes the White Paper is going to attach to an organization.

00:21:49 Speaker 4

A publication is going to attach to a journal or conference of some form.

00:21:59 Speaker 4

If they just give you a title.

00:22:02 Speaker 4

Then you go hunt through Google for that title.

00:22:06 Speaker 4

Or you do in exact search.

00:22:09 Speaker 4

But generally you look for the person you look for the publication title and you look for it in the places they say they're published.

00:22:17 Speaker 5

OK.

00:22:17 Speaker 5

And so if we're, if we want to check the individual's credentials, I imagine it's exactly the same. We're going to go and, like check specifically with the university.

00:22:25 Speaker 4

Yeah. Well, if they're a university researchers, sometimes, I mean, you get researchers in large organizations as well, like tech organizations have researchers.

00:22:26 Speaker 5

Feel this?

00:22:37 Speaker 4

They're they're a little harder. They're a little more.

00:22:41 Speaker 4

But again, you can you can look them up. Researchers don't tend to come out of nowhere. They tend to have a research history. They tend to have collaborators you can check.

00:22:58 Speaker 5

So these are super simple, but we would flush these out and so.

00:23:06 Speaker 5

Yeah, so our fake experts, what do we want to do? We have two tasks here as we just said, check with the publisher and then check the credentials with the university. But maybe that's not good enough. Maybe we need to dig deeper. We could mention a task for checking if they're on less reputable.

00:23:25 Speaker 5

Versus that might be interesting or has any of their material been distributed?

00:23:38 Speaker 5

Like sites that pirate academic papers or something like, is there a kind of like out of band channel, you know, where we might find this that you know is interesting?

00:23:51 Speaker 5

And so yeah. So anyways, like for however, we want to verify this, we just build up the steps and then organize it into buckets like verification might make sense as a title. It might be something else. And that's really.

00:24:06 Speaker 5

All. All we have to do with these case workflows, they're super simple and then we save it.

00:24:15 Speaker 5

Now we have a new case template over here. So to actually use this and merge it into an ongoing investigation, let's first create a.

00:24:27 Speaker 5

A new investigation for our purpose here so demo.

00:24:33 Speaker 5

We create our case.

00:24:40 Speaker 5

So this uses the base template that I mentioned previously, like it tells us, you know, create an event, create a Deccan, whatever.

00:24:51 Speaker 5

And now we create the new workflow we're interested in. So use fake experts.

00:25:04 Speaker 5

We go back to the main view. These are our two cases and we merge them. So we select the original case, select merge over here.

00:25:15 Speaker 5

And then.

00:25:22 Speaker 5

The new workflow we created is that the case.

00:25:30 Speaker 5

And that's it. So we have all of the original base template case, you know like create the music events and additionally under tasks.

00:25:40 Speaker 5

We have the base tasks initialization plus the verification tasks for.

00:25:47 Speaker 5

Finding out publisher and whatever else.

00:25:53 Speaker 5

So that's how you do it in the platform. That's kind of what we're working.

00:25:56 Speaker 5

With and. The reason I lead with the question about, you know, like whether this is appropriate.

00:26:01 Speaker 5

Is it's a little clunky and it's going to take.

00:26:06 Speaker 5

A patch to make this you know smoother and less painful. And so that's something I think we need to think hard about and actually really.

00:26:14 Speaker 5

Practice as a team. Make sure like.

00:26:17 Speaker 5

[Name redacted] and the folks that are doing the triage are comfortable and like this. If they don't, or if it's slow, it doesn't make sense to go out and build, you know, like.

00:26:28 Speaker 5

Workflows for everything we're not like.

00:26:31 Speaker 5

You know, we're not set. It's not set in stone that we have to use this. We can use anything we want. So we should, you know, pick whatever makes our life easier.

00:26:38 Speaker 5

UM.

00:26:41 Speaker 3

That is awesome for women. Do you have any last thoughts, [Name redacted], before we toss it out to everybody to ask some initial clarifying questions?

00:26:51 Speaker 5

No, I think I think I.

00:26:52 Speaker 5

Got everything out there.

00:26:53 Speaker 3

Awesome. Cool. So now we'll take a few minutes just to do clarifying questions for those who are new to the game. This is like, yes, no questions, few word, answer kind of thing that you'd like. A quick response from [Name redacted] on to better understand it. So then we can ask more probing questions later.

00:27:13 Speaker 7

I have a quick question. Hi everyone. I'm [Name redacted]. I'm I'm new to CI league. I'm a red teamer at [company redacted]. I was wondering is this, is there an existing sort of like database or library with with existing templates?

00:27:35 Speaker 7

Or or is this all?

00:27:36 Speaker 7

Kind of being made on the fly.

00:27:39 Speaker 3

Great question.

00:27:41 Speaker 5

Yeah. Hi, [Name redacted]. Welcome. So there is.

00:27:48 Speaker 5

They're mostly like Infosec malware type, A situation focused. So there's a really interesting project out there. It's called atomic threat coverage.

00:28:01 Speaker 5

And what they do is they generate that dynamically generates hive case templates.

00:28:08 Speaker 5

Using Sigma rules and.

00:28:14 Speaker 5

Atomic Atomic Red Team output of of that project.

00:28:20 Speaker 5

And so that's a really interesting use case. Unfortunately, nothing like that really exists for this info, but I modified atomic threat coverage a few months back to support the emit framework, as well as some of the language we're likely to use in the future. And.

00:28:38 Speaker 5

So if we.

00:28:39 Speaker 5

Do you go down that route? If we find out like sources that are appropriate for use there, we could do the same thing.

00:28:47 Speaker 3

And to clarify, [Name redacted], Amet is like the disinformation version of MITRE, which I believe was created by [Name redacted] and [Name redacted].

00:29:00 Speaker 1

Sort of. So Amit is the misinformation version of attack, which is the framework created by Mitre to describe cybersecurity incidents. And [Name redacted] and I and a few more married men and women created it.

00:29:18 Speaker 1

About a year and a half ago.

00:29:20 Speaker 4

Yeah. We let a band of people.

00:29:22 Speaker 4

Putting it together.

00:29:24 Speaker 4

So [Name redacted] and I sat in a room and yelled at each other until we got it right.

00:29:31 Speaker 1

For literally weeks.

00:29:34

Yes, [Name redacted].

00:29:37 Speaker 7

No. Yeah. No, thank you for answering that question. That's really insightful. I wasn't aware of this, so thank you.

00:29:47 Speaker 3

Awesome. Any other clarifying questions before we dive into probing?

00:29:59 Speaker 3

I guess one clarifying, no, sorry, one clarifying question I have for you, [Name redacted].

00:30:02 Speaker 3

Is in places where this is kind of working smoothly.

00:30:06 Speaker 3

What is the?

00:30:07 Speaker 3

Type of interaction that people have with this.

00:30:15 Speaker 5

Yep. So in most cases, case in most organizations I've worked with and where I've deployed HIVE or built out to link for the Hive, this case management workflow is not standard. It's too complicated and it's too slow. But it it's my opinion that this is the correct.

00:30:31 Speaker 5

Way to do it.

00:30:33 Speaker 5

And that we should work towards.

00:30:35 Speaker 5

Making this.

00:30:36 Speaker 5

Making this easier.

00:30:39 Speaker 5

But how it's typically used is optimizing for speed. The hive should make it quick for you to enter data, run cortex analyzers that return results from virus total or your own custom integrations so that you can read that data and take decisions.

00:30:58 Speaker 5

From it.

00:31:01 Speaker 5

That's how it should be used, and that's even how the devs promote its use.

00:31:08 Speaker 5

For us it's a little.

00:31:10 Speaker 5

There's a little work to do to speed up getting that data in.

00:31:14 Speaker 5

And also to handle the the data types we're interested in. So I'll I'll show you what I'm talking about.

00:31:23 Speaker 5

The default observable types are. All are all atomic indicators like you know.

00:31:30 Speaker 5

IP address or a file hash, but something like a A A Twitter post which itself you know is a collection of all of these different things, like a user name and text and timestamp and whatever can't be represented. We can only represent these atomic indicators. And so that's kind of that's kind of a failing right out of the gate.

00:31:50 Speaker 5

We want to work with those we need.

00:31:54 Speaker 5

Some integrations to handle that, and like extract those interesting bits and then.

00:32:00 Speaker 5

Flattened them, or I know [Name redacted] has worked on.

00:32:05 Speaker 5

A method to include like parent objects and make them more complex. It's another option.

00:32:13 Speaker 5

So I think I'm kind.

00:32:14 Speaker 5

Of getting off topic here but.

00:32:18 Speaker 5

Did I answer you? Let me just stop. Did I answer your?

00:32:21 Speaker 5

Question yeah.

00:32:22 Speaker 3

Yeah, I think so. Let's toss it open to just broader questions. You have anything that pushes on the assumptions wants to get at a deeper question here.

00:32:33 Speaker 6

And one question I have just is the relationship between this and MISP and when we talk about this group and going through triage is, is the idea that hive is the the primary entry point that we go in and then the information flows through there or what's what's that interaction?

00:32:54 Speaker 6

What do you think about?

00:32:56 Speaker 5

So have you missed as a record of authority, we use it.

00:33:02 Speaker 5

To present public facing threat intelligence like we create a report we're happy with how it looks. We go and push it out to the community so they can ingest it and and and trust.

00:33:13 Speaker 5

Everything in there is appropriate meets some minimum standard or whatever. Hive is really just like where we get work done, we can.

00:33:22 Speaker 5

Junk in here? That's totally OK. Run cortex analyzers to enrich it. Work through our findings. And then when we're happy with the results or when we're happy with, you know, some set of the results push.

00:33:37 Speaker 5

That, you know, only the things which.

00:33:40 Speaker 5

We're happy about back out to MISD.

00:33:44 Speaker 5

And right now that's like a.

00:33:46 Speaker 5

Partially manual process I.

00:33:49 Speaker 5

I wrote a I wrote an integration for Hive that.

00:33:55 Speaker 5

Allows us to export.

00:33:59 Speaker 5

Case observables as well as tags and Emmitt.

00:34:06 Speaker 5

Amid galaxies or?

00:34:09 Speaker 5

Yeah, and galaxies and MISP back out.

00:34:11 Speaker 5

To MISP.

00:34:12 Speaker 5

So the default integration, there's a default integration, you can go to.

00:34:21 Speaker 5

Where is it? There's like an export feature.

00:34:25 Speaker 5

It's not configured on this one so.

00:34:28 Speaker 5

OK, so to answer your question about Hive and MISP, there's a default integration that allows you to export only some sets of observables. For our purpose that wasn't going to work and so I built a custom one that allows us to export everything.

00:34:40 Speaker 5

And we do that here under responders select MISP.

00:34:45 Speaker 5

And it just runs, it'll export the the case, the title, all of the.

00:34:51 Speaker 5

Observables that are in this case, along with the tags that are here and the tags.

00:34:57 Speaker 5

On the individual observables themselves, so that saves us a lot of work.

00:35:02 Speaker 5

But the problem the thing we need to think about is.

00:35:07 Speaker 5

All of these exported observables are flat, you know, so it's a Twitter URL. It's not the same as a Twitter object in this.

00:35:14 Speaker 5

And we're going to have a lot of junk in here that we don't want to send. And the way I currently handle that is by marking individual.

00:35:25 Speaker 5

As IOC's.

00:35:29 Speaker 5

So each observable here has the star. It's an IOC tag and that tells us it's.

00:35:36 Speaker 5

It's an indicator that you know isn't providing correlation or isn't a false positive or whatever. It's actually something we're interested in that we want to share.

00:35:44 Speaker 5

You know, it actually indicates compromise or a disinformation or whatever.

00:35:49 Speaker 5

When when this flag is set and we run the cortex or responder.

00:35:55 Speaker 5

Only this user name in this case only this observable that's marked will be exported.

00:36:00 Speaker 5

Out from this?

00:36:02 Speaker 5

So that's in there now.

00:36:08 Speaker 5

Did that answer your question?

00:36:10 Speaker 6

Yeah, definitely. Thank you.

00:36:11 Speaker 5

OK, cool.

00:36:15 Speaker 3

Other questions? [Name redacted] [Name redacted] [Name redacted].

00:36:20 Speaker 4

So we have a bunch of things we used to put.

00:36:22 Speaker 4

Into MISP. So we've been uploading straight up from Slack to MISP.

00:36:29 Speaker 4

But we're talking about MISP as being the how did you put it? The objects of record?

00:36:38 Speaker 4

So how are we going to square that?

00:36:44 Speaker 4

I like by the way, the upload to to miss from from Hive. That's that's nice.

00:36:51 Speaker 5

Yeah, I need to.

00:36:53 Speaker 5

Need to do some more work so that if we.

00:36:57 Speaker 5

Have a Twitter username or like a Twitter URL rather than adding a atomic indicator, it actually goes and queries the Twitter API to pull out all that additional data and create a missed object. And that's something I can do. I just need to find the time to do it.

00:37:12 Speaker 5

Let's answer your first question about how we how we square away our current working with Miss and kind of where we want to.

00:37:21 Speaker 5

I don't see a problem with like our previous work in Miss. Some of our events, you know it's a learning curve we've.

00:37:25 Speaker 5

Put together data.

00:37:29 Speaker 5

That points to a point to like a problem, but I think going forward as we kind of refine our processes that we want to be a little more conservative in what we send in, like if we're tracking.

00:37:43 Speaker 5

You know, we're tracking the the UM.

00:37:48 Speaker 4

Well, let's think about the million masks million mask incident. So we've got a bunch of stuff that's related to it, some of stuff which.

00:37:54 Speaker 4

Might be related.

00:37:55 Speaker 5

To it. Yeah. So so for miss.

00:38:00 Speaker 5

Sorry, go ahead.

00:38:01 Speaker 4

I was going to say we we want to keep those objects somewhere so that we can see them if they turn up.

00:38:08 Speaker 4

Again, for example, the admins on that Facebook page.

00:38:12 Speaker 4

If they turn out to be admins we've seen on earlier pages on earlier marches and Springfield, IL is kind of a hotspot. So if we've got the same people keep doing.

00:38:23 Speaker 4

The the thing.

00:38:25 Speaker 5

So there's there's no issue putting.

00:38:29 Speaker 5

Of casting a wide net for some missed events, as long as we mark them as such. You know, like for the lockdown or for the the mask incidents.

00:38:39 Speaker 5

Keeping the you know the page admins keeping individuals that are posting about it, but we suspect they're interesting is totally fine. I just want to. I just want to avoid posting adding to MISP every single user that like retweets something and that person is insignificant in the grand scheme of things. You know, like if we if we suspect, OK. So if that's not happening.

00:38:56 Speaker 4

That doesn't happen.

00:39:00 Speaker 5

It's not an issue.

00:39:02 Speaker 4

So it's about what are the boundaries in what we put in.

00:39:06 Speaker 4

Sometimes we're going to have 100 different sites when we chase the boogaloos, we found 200 different different groups.

00:39:11 Speaker 5

Yeah. Or pay.

00:39:14 Speaker 5

Pink slime as well. You know you had you.

00:39:16 Speaker 5

Had so many.

00:39:16 Speaker 4

Yeah, yeah.

00:39:18 Speaker 4

So some of them are going to be pretty big because they need to be big to tell.

00:39:22 Speaker 4

People about the whole group.

00:39:26 Speaker 4

I am trying to bottom out what the issue.

00:39:31 Speaker 4

With what you put in Misfits.

00:39:34 Speaker 4

So if we just continue doing what we do, which is post ally related data up to nisp.

00:39:42 Speaker 4

We may have to do things in the other direction, and if we're posting from Slack to Misp is then bring it back from misp over to Hive.

00:39:51 Speaker 5

I'll give you. I'll give you a good a good example. So when we have.

00:39:58 Speaker 5

You know, when we looked at the lockdown sites we had, like [Name redacted] and [Name redacted] and some folk.

00:40:05 Speaker 5

Pull out Maltego transforms and look at like the hosting providers and domains that are hosted on those IP addresses. There's a lot of noise you could do that automatically in hive. You could build a cortex analyzer that does that work and returns it into a workflow so that you could browse that finding right. So there's a lot of data in there.

00:40:25 Speaker 5

A lot of it's going to be junk. Totally not appropriate for MISP, but once you identify the things that are interesting out of that, you mark it as interesting and then you can export it out to MISP. But that would be like 1.

00:40:38 Speaker 5

That would be 1 like.

00:40:42 Speaker 4

That works with pink slime as well, because if you're doing a built with trace.

00:40:47 Speaker 5

Yeah, exactly.

00:40:47 Speaker 4

Quite often you're going to get a bunch of sites that the other the people just.

00:40:52 Speaker 4

Happen to have built.

00:40:53 Speaker 5

Yeah, I made that.

00:40:54 Speaker 4

And use syntax.

00:40:56 Speaker 5

I made that mistake with the built in Slack bot. I I created it, it ended up sending it a ton of junk to this.

00:41:04 Speaker 5

So like I mean to answer this, the spirit of of your of your question, I don't have a like a I don't have a.

00:41:12 Speaker 5

100% way to nail this down. It's it's arts as much as science, so it's up to us to, you know, kind of use our discretion and and figure out.

00:41:24 Speaker 5

How much noise is appropriate for our disinformation? Consider that we're sharing, you know what the boundaries are so.

00:41:30 Speaker 4

I I think the answer seems to be that we run the automated stuff and get the automated responses in HIVE, but the hand curated stuff goes up to miss.

00:41:42 Speaker 5

I I think our team too like you know it's.

00:41:45 Speaker 5

We have.

00:41:47 Speaker 5

You know, we have a solid team and it's been pushing forward a lot of interesting data and I think like.

00:41:56 Speaker 5

What they select to share with us in the channel tends to be pretty relevant. You know, it's not a lot of garbage.

00:42:03 Speaker 5

And so, you know, because of that a lot of relevant stuff ends up in missed. And I think as long as we can maybe continue to create that culture of like making sure people stay on points, understanding what's kind of you know reasonable to assume is relevant, then we're good. You know if we grew like you know exponentially over the next few days we might have problems.

00:42:25 Speaker 4

We make sure it goes in.

00:42:26 Speaker 4

The training.

00:42:27 Speaker 4

And basically as part of the training is we're looking for things that are connected just.

00:42:33 Speaker 4

What is of interest to somebody who's analyzing this thing?

00:42:36 Speaker 3

Yeah, and this is perfect. We've transitioned right into the discussion.

00:42:40 Speaker 3

This is great.

00:42:44 Speaker 3

Cool. So to bring us back to [Name redacted]'s initial question is so is, does this seem to be the right tool for case management for us or for incident management for us? And if so, what are the types of things that would make life easier in here for you guys, for people who are?

00:43:01 Speaker 3

Using this all the time.

00:43:06 Speaker 4

I hate really, really, really hate those merges.

00:43:12 Speaker 4

Yeah, they mess up the numberings. I mean, it's not so bad. It's not because the missed numbers we we use for the uploads. So we need them. So it's not so hard finding the.

00:43:25 Speaker 4

Type stuff again.

00:43:28 Speaker 4

It's it's difficult, it's messy when you do emerge. You. I mean, if you've got two URLs you're chasing.

00:43:37 Speaker 4

And a set of tasks on the.

00:43:39 Speaker 4

There's no sense of which tasks go with which URL.

00:43:45 Speaker 5

Yeah, I yeah, I I totally agree. It's.

00:43:48 Speaker 5

It's ugly, but they're, I added I actually.

00:43:54 Speaker 5

Added onto the.

00:43:56 Speaker 5

Hackathon notes like a request to either create proper sub cases or merge natively and.

00:44:06 Speaker 5

Again, not ping [Name redacted] about that. It might be something.

00:44:11 Speaker 5

His team has has the skills to produce for us, and if that's the case.

00:44:19 Speaker 5

We should just have a.

00:44:20 Speaker 5

Conversation about what? The.

00:44:21 Speaker 5

Ideal case template would look like or what the ideal organization would look like. Do you prefer something like you know, actual?

00:44:31 Speaker 5

Sub cases you know, like could we do so right here we have a list of tasks, right? If we had like another tab here with like.

00:44:40 Speaker 5

You know, like sub subcases or whatever. We open that up and inside.

00:44:44 Speaker 4

That would be.

00:44:44 Speaker 5

Of it, we.

00:44:44 Speaker 4

Nice. We have stuff for those, yeah.

00:44:45 Speaker 5

Have we have?

00:44:45 Speaker 5

Tasks here, but we keep.

00:44:48 Speaker 5

It all, you know, organize. You would know what goes with what and that's that's your main problem is.

00:44:52 Speaker 5

That this gets.

00:44:53 Speaker 5

Jumbled up, right.

00:44:55 Speaker 4

You don't know what goes with what. It's it's. I mean, it's unusable for me. I just. I can't use this.

00:45:01 Speaker 5

OK.

00:45:03 Speaker 4

So that having a tab with the subcases would make life a lot nicer.

00:45:09 Speaker 4

Having those marked so they're not coming up with the same response.

00:45:15 Speaker 4

There are other things we want to put into to fix on hive as well, like the. If you do A tag search.

00:45:24 Speaker 4

It's an or. It's an or search, not an and search.

00:45:29 Speaker 4

So it's been annoying me horrendously that I look up disinformation incident.

00:45:34 Speaker 4

And I get all of the cases for disinformation, plus all of the cases for incident.

00:45:40 Speaker 4

Not all of the cases for disinformation and incident.

00:45:44 Speaker 5

OK. Like I'm noting that down as you're speaking and that's, I mean, I don't want to speak for [Name redacted], but that doesn't.

00:45:51 Speaker 5

Sound like a complicated change? I'm pretty sure it's something we we could reasonably request.

00:45:56 Speaker 4

I think that that may be.

00:45:56 Speaker 3

Awesome. And I'm also taking notes. I'm also taking notes right in the in.

00:45:59 Speaker 3

The doc that.

00:46:00 Speaker 3

We have too the slide deck. Sorry to interrupt.

00:46:09 Speaker 4

Yeah, I think you've hit that. That's hit all the things that really annoy.

00:46:12 Speaker 4

Me about hype.

00:46:14 Speaker 4

I mean, there's some stuff like, you know, we're we're trying to work together and it's still easier to use a Google Doc.

00:46:21 Speaker 5

Honestly, yeah, here's another another major consideration is that.

00:46:31 Speaker 5

The the reason we're doing this, I think or.

00:46:36 Speaker 5

One of the major reasons is the assumption that we'll use cortex analyzers for automating the manual things we're doing.

00:46:43 Speaker 5

You know, like those multiple transforms or looking up who is or something. So far we haven't really built any of those or haven't built any ones that are useful or that I see being used on a day-to-day basis.

00:46:56 Speaker 5

And if we can't go out and identify a a reasonable set of cortex analyzers and and we can't identify things that can actually be automated, you know, in in relation to in information operations, then we might want to, you know, consider whether or not this this makes sense like.

00:47:15 Speaker 5

Cortex is a huge selling point of this system. If all we're using it for is strictly case management, well, there are, you know, there are 100 case management systems out there.

00:47:26 Speaker 4

We've been using the case management because it's so difficult to use sub cases.

00:47:32 Speaker 4

It really is horrible if we can fix that the the other thing that I would like to have if you're asking wish.

00:47:32 Speaker 2

You know.

00:47:34 Speaker 3

Yeah. So.

00:47:41 Speaker 4

Lists. Yeah, yeah, yeah.

00:47:43 Speaker 4

Is we're having long conversations and slack, we've managed to get people threading those long conversations about cases.

00:47:51 Speaker 4

We just pick up those slack threads and throw those into the cases.

00:47:56 Speaker 5

Oh, that's an easy one, actually. Like to probably bang that out in an afternoon.

00:48:01 Speaker 4

Yeah. So just as we're writing what we find in the slack.

00:48:02 Speaker 5

Let me just.

00:48:07 Speaker 4

We could post that over to the case so it just.

00:48:09 Speaker 4

Gets copied over.

00:48:13 Speaker 3

This is why we're.

00:48:13 Speaker 3

Having this conversation, this makes me so happy.

00:48:15 Speaker 4

Yeah. Well, I'm thinking ahead to when other teams are reading our hive as well. So we're we're not sharing just with ourselves, but we've also got the other CTI teams and possibly external teams looking at our case notes.

00:48:19 Speaker 3

Right.

00:48:29 Speaker 5

Just for the slack to Hive Bot, would it be acceptable to do something like start a thread?

00:48:39 Speaker 5

Tag it or Mark it somehow like maybe like a boilerplate initial post. You know, like, you know, like a text that says hey, trigger Slack bot case ID or whatever and then after that the slack bot just reads every comment in that thread and pushes it out to the hive. You know case.

00:48:59 Speaker 4

So start hive number.

00:49:05 Speaker 5

Actually, maybe you could just, maybe you could just.

00:49:08 Speaker 5

Call the slack bot within the thread. I'm not really sure if the slack bot knows what thread it's living in, but that might be an option too, so.

00:49:15 Speaker 6

Yeah it does. You can do that.

00:49:17 Speaker 5

Yeah. OK, cool. So that's that's the answer then.

00:49:19 Speaker 4

I'm a bit like a thread thread thread on roller. Yeah, you're basically doing a thread on roller in, in, in, in slack and checking it over to hive.

00:49:22 Speaker 5

Yeah, cool.

00:49:29 Speaker 5

Yeah, I'll add it to that. I'll add that to the pathon because that's that's an easy one.

00:49:38 Speaker 3

I guess one thing I'd be interested to dig into a bit more and I don't have the expertise to actually get into the pieces of it would be, are there things that we would prioritize automating using the cortex analyzer like if that's the thing that really is the unique value proposition of this tool, what are the things?

00:49:55 Speaker 3

That we would hope to automate.

00:49:58 Speaker 3

That we'd want to build out.

00:50:01 Speaker 4

OK so.

00:50:04 Speaker 5

Let's try to take.

00:50:05 Speaker 4

It away I was going to say as the person seems to be.

00:50:08 Speaker 4

Doing a lot of the.

00:50:10 Speaker 4

The the Data Nerd Inc.

00:50:13 Speaker 4

So we get a URL.

00:50:15 Speaker 4

We want to know who owns that URL and which.

00:50:21 Speaker 4

Other URLs are connected to it through things like add tags. So we run built.

00:50:24 Speaker 4

With and find.

00:50:24 Speaker 4

That we run the DNS checks on it.

00:50:29 Speaker 4

So it's OK, you've got a URL. Let tell me more about this spider out from this URL. Find other URLs connected to it.

00:50:39 Speaker 4

We've got.

00:50:41 Speaker 4

The other thing with the URL is you want to go see who's referenced it. So lookout on social media for it.

00:50:48 Speaker 4

So you're gonna go hunt. See where in Facebook's mentioned it. You wanna go hunt to see where in Twitter?

00:50:57 Speaker 4

Instagram wherever.

00:51:00 Speaker 4

There there's hashtags.

00:51:03 Speaker 4

You get a hashtag you want to.

00:51:05 Speaker 4

Go look for.

00:51:07 Speaker 4

Everything on that hashtag. So you want to just pull?

00:51:12 Speaker 4

Who in the last week or you know, going back time span of interest.

00:51:19 Speaker 4

Who's talking about it? How are they connect to each other? What are the Super nodes in that network? What are the hashtags are with it?

00:51:27 Speaker 4

You want to look on.

00:51:30 Speaker 4

Face on Facebook, which groups are talking about it again? What else is with it? What phrases are with it?

00:51:42 Speaker 4

If you look at Facebook pages, this is thing I've been I've been building for two bloody log and I can hand over to the hackathon I've done.

00:51:49 Speaker 4

Is you get when you look at a page, you also get pages related to this.

00:51:56 Speaker 4

And you can spider down through those and and find a whole bunch of connected connected groups. That's how we found a bunch of.

00:52:04 Speaker 4

The boogaloos.

00:52:05 Speaker 3

Awesome. So in some ways, you're kind of describing some of the things that we initially built out in the big book as kind of like step.

00:52:11 Speaker 3

By step process.

00:52:12 Speaker 4

It's literally, but that's why we wrote them up in the big book is to train people, but also to automate.

00:52:17 Speaker 3

OK.

00:52:22 Speaker 4

It's like, how do you scale what one or two analysts do to lots of people and to do it quickly?

00:52:32 Speaker 5

You can say. Here's here's a thought on that too. So one of the one of the failings here.

00:52:40 Speaker 5

Of cortex or.

00:52:43 Speaker 5

One of the limitations, let me show you.

00:52:47 Speaker 5

So that when we.

00:52:49 Speaker 5

Creates when we run a cortex analyzer.

00:52:54 Speaker 5

I don't think any of these will return interesting results, but when we run a Cortex analyzer, it returns a.

00:53:03 Speaker 5

HTML report. So it's like HTML plus J2 templating.

00:53:12 Speaker 5

Which is OK for if we can like.

00:53:15 Speaker 5

Put that data in cells you know we can build a tabler or whatever.

00:53:21 Speaker 5

But for very large amounts of data or.

00:53:25 Speaker 5

You know.

00:53:27 Speaker 5

Something that's better represented in a network. This isn't. This isn't great. So.

00:53:32 Speaker 5

Maybe we could.

00:53:33 Speaker 5

Add something like a Jupyter notebook integration into Hive. That might be interesting for the.

00:53:40 Speaker 5

For for these, for many of the use cases you just described, it sounds to me like you know this format wouldn't really help you. You'd end up exporting that data elsewhere to actually evaluate it, and if that's the case, then this tool failed you in the 1st place. You shouldn't have to make extra steps, should be.

00:53:56 Speaker 5

Saving your work so.

00:54:00 Speaker 5

I'll add that to the I'll add that to the to the list and and actually maybe that even solves our Web app Jupyter notebook problem as well if we can just embed them here.

00:54:12 Speaker 4

Let's let's work on that. We need Jupyter notebooks for the the.

00:54:16 Speaker 4

Other work we're doing.

00:54:17 Speaker 4

And we've got a whole bunch of stuff we haven't pulled over.

00:54:20 Speaker 4

From data science yet.

00:54:24 Speaker 3

Awesome. Any other ideas? [Name redacted]? [Name redacted]. [Name redacted]. Anybody who hasn't jumped in yet?

00:54:32 Speaker 6

And I was thinking about the relationship with, you know, Cortex and data analysis. [Name redacted], you said that the data that comes back from Cortex into hive is just the HTML templated stuff or is it the JSON and a template that gets transformed into HTML?

00:54:48 Speaker 5

Yeah, it's JSON that gets transformed into an HTML J2 template.

00:54:53 Speaker 6

OK, so I can also imagine you know whether or not it's built into this something, you know, a small tool that we can pull up a case in hive and then go to cortex and say show me all the jobs that were run related to this incident and then give me all that data or something like that.

00:55:12 Speaker 5

Yeah. So that's totally a that's totally A use case.

00:55:17 Speaker 5

Cortex has, like Cortex, has a rest rest API and you can configure it to send web hooks. Whatever job is executed and so we could like branch that or like split that data out so it's sent to another service that does whatever easily and that's actually something I do.

00:55:38 Speaker 5

Day job. We like send it out to our data lake and to like nifi and whatever where we do transforms on that for.

00:55:49 Speaker 5

So there's a lot of flexibility there and you can just query cortex directly, if that's your thing.

00:55:55 Speaker 6

Well, then another another question that was mentioned on Deccan and still haven't looked too much in it yet, but have there been any thoughts about you know the whole export to Deccan for whatever you use cases?

00:56:09 Speaker 5

I haven't touched it.

00:56:12 Speaker 5

It's on our list.

00:56:13 Speaker 5

But I haven't touched it. And again I guess that's.

00:56:16 Speaker 5

One from the hackathon.

00:56:19 Speaker 4

Oh, we've lost [Name redacted][Name redacted] is decamp person.

00:56:23 Speaker 6

Got it. I'll admit that was kind of a leading question to learn a little bit.

00:56:26 Speaker 6

More about.

00:56:26 Speaker 3

Deccan too.

00:56:32 Speaker 4

Has [Name redacted] done the decant training or we yet to run?

00:56:34 Speaker 3

That, yeah, couple, maybe two weeks ago. I think we do have a recording.

00:56:35 Speaker 5

You said it.

00:56:39 Speaker 3

Of it that we can put up.

00:56:41 Speaker 6

Yeah, I missed that. So if we can link me to that.

00:56:43 Speaker 3

That'd be awesome. Totally. Once we we're just kind of hunting down the recordings because different people zooms have the recordings. So once we hunt all those down, I'll link them into a.

00:56:52 Speaker 3

Dock and then share them with you.

00:56:58 Speaker 7

Yeah, I would.

00:56:59 Speaker 7

Really appreciate that that would that would be great.

00:57:04 Speaker 6

The other thing I'll mention that there was a conversation about, you know, pulling stuff out of threads. I do have that bot that I prototyped the, you know, we'll take a thread as long.

00:57:14 Speaker 6

As it's pinned.

00:57:16 Speaker 6

Pull it and start extracting all of the at least the URLs at this point, but it's a good shell.

00:57:22 Speaker 6

At least you know, figuring out where Slack API is, what the data structures.

00:57:27 Speaker 6

Look like and.

00:57:27 Speaker 6

It might be a decent starting point for doing some pulling stuff out.

00:57:33 Speaker 6

Read one thing that.

00:57:35 Speaker 6

I thought about in doing that is there's you can have a slack bucket notifications when certain emojis are used and we could come up with patterns to the, you know emojis have different meanings or something like that as well.

00:57:52 Speaker 4

Australia added MISP and hive emojis to the set of emojis we've got, so we've been using that to mark where we've put something in Mr. Hype.

00:58:04 Speaker 6

That might be a perfect trigger.

00:58:17 Speaker 3

Any other thoughts?

00:58:19 Speaker 3

Oh, sorry so much about to jump in.

00:58:21 Speaker 5

Yeah, just a question for [Name redacted]. So that's slack bot. Is it in the CTI league, whatever Git, GitHub.

00:58:30 Speaker 6

It's not yet I I actually that's on my To Do List. To do that I should do that immediately because the only other git repo as it is is in the Heroku instance. So I I'll prioritize that.

00:58:43 Speaker 6

In the next.

00:58:43 Speaker 5

Yeah, yeah. No, no rush. I'm not going to have time to look at it for the next few days anyways, but when you.

00:58:49 Speaker 5

Can I'm curious to. I'm gonna be looking OK.

00:58:51

Take a look.

00:59:00 Speaker 3

Any last thoughts before we toss back to [Name redacted] for?

00:59:04 Speaker 3

Any reflections I forgot? Wait, what did I call this next section responses. Yeah.

00:59:13 Speaker 3

So anything you're thinking about [Name redacted] in terms of your next steps based?

00:59:17 Speaker 3

On this conversation.

00:59:23 Speaker 5

Yeah. So my next.

00:59:23 Speaker 3

Most, I guess anything that was most helpful to you is.

00:59:25 Speaker 3

Another way to think about that.

00:59:27 Speaker 5

The most helpful thing is is confirming my suspicion about the the friction of using the platform as to answer that for me and so my next step I need to build out the the required tooling, get the features we need pushed upstream or to our own custom branch. If we can't do that.

00:59:47 Speaker 5

Or if we run into like some unforeseen issues, then we need to reconsider what we're using for case management.

00:59:55 Speaker 5

I think, but I also you know I think.

00:59:57 Speaker 5

We can solve those problems.

01:00:00 Speaker 3

Cool. And then maybe a quick brief just if folks want to go around and just really quickly like what worked about this structure of like this is a debrief on the protocol, not a debrief on the content, but we can do both. So what worked for you? Is there anything you tweak for next time, just want to kind of?

01:00:20 Speaker 3

Get a sense of.

01:00:22 Speaker 3

Moving together and having processes for that.

01:00:27 Speaker 4

I I guess I'll start. I like the protocol. I like the fact that we move to different types of questions. It's it's useful, nicely put together.

01:00:38 Speaker 4

UM.

01:00:41 Speaker 4

Need to frame the type of talk it is.

01:00:45 Speaker 4

So this one was very much about we have this thing. What do we need to do to it rather than a very basic training in in what hivis?

01:00:56 Speaker 3

Awesome, really good.

01:00:56 Speaker 4

So we perhaps need to mark up levels.

01:01:00 Speaker 3

Good call out.

01:01:04 Speaker 6

I like. I like the format and also that clarifying about you know clarifying questions because the I think the first one of these I completely went over my head of what that should have been and I think it wasted a lot of time and echo what as Jay said as well about more context about what this is because they can.

01:01:24 Speaker 6

Also, maybe invite different types of people.

01:01:27 Speaker 6

In the conversation too.

01:01:50 Speaker 3

And for me, my constant reflection is when do I shut up and when do I talk? I think someone else was.

01:01:56 Speaker 3

Just about to talk.

01:01:57 Speaker 3

And then I started talking again.

01:02:03 Speaker 3

I'm just watching the meetings.

01:02:06 Speaker 3

Any last thoughts, [Name redacted]?

01:02:09 Speaker 5

I like this format and I like how you moderate the chat. I think it's important that you're making sure folks aren't being spoken over something doesn't go on like a.

01:02:22 Speaker 5

15 minute tirade.

01:02:26 Speaker 5

Partially talking about myself there and yeah, you know.

01:02:29 Speaker 5

So like I.

01:02:30 Speaker 5

Like this, keeping people on track, making sure like we have focus on different types of questions. This feels correct to me.

01:02:41 Speaker 3

Awesome. And if you guys have any other feedback from me, I'm always open to it. Just let me know and we'll keep it moving.

01:02:50 Speaker 3

Cool. And we ended a minute early.

01:02:52 Speaker 3

Any last thoughts before we jump?

01:02:54 Speaker 5

We have the Red Team meeting now and folks. Yeah, folks on this call, folks on this call are welcome to join.

01:02:56 Speaker 4

Yeah, it's not a joke.

01:03:02 Speaker 5

I'm not sure.

01:03:03 Speaker 4

Sorry, what is that?

01:03:04 Speaker 4

OK, so basically we did some red teaming for disinformation a while back and we had so much fun doing.