Audio file

2020-05-16_TeamMeeting_Training_[Name redacted]OnTTPs.m4a

Transcript

00:02:40 Speaker 2

[Name Redacted], how are you, Sir?

00:02:42 Speaker 1

You know another day.

00:02:45 Speaker 1

Another chance to swear at some computers.

00:02:48 Speaker 2

I hear you.

00:02:51 Speaker 1

Let's make sure before we.

00:02:53 Speaker 1

You'd go on, then. [Name Redacted] didn't change the link.

00:02:56 Speaker 1

On us again.

00:02:58 Speaker 1

Or [Name Redacted].

00:03:02 Speaker 3

Whoops, not not that one.

00:04:24 Speaker 1

Good. I'm not the only one. Awesome. Thank you, [Name Redacted], for putting that in Slack.

00:04:31 Speaker 2

Yes, Sir. [Name Redacted] just asked me to.

00:04:33 Speaker 2

Do that.

00:04:34 Speaker 4

Hey, guys.

00:04:36 Speaker 2

What's up, [Name Redacted]?

00:04:41 Speaker 4

We are not much.

00:04:46 Speaker 4

Should we have in here?

00:04:47 Speaker 4

So far, just just us.

00:04:51 Speaker 2

Nobody here but us chickens.

00:04:56 Speaker 1

Nobody here or nothing going on. No pay attention, it's.

00:05:14 Speaker 1

And it if it gives you any indication how much it it gives you a good indication of how much adventures of Rocky and Bullwinkle I watched as a child and then I can go straight into.

00:05:23 Speaker 1

The Boris accent no problem. Most sense squirrel.

00:05:26 Speaker 2

I know there's a reason that we get along.

00:05:34 Speaker 1

I caught [Name Redacted] watching that the the new version, at least on his little fire tablet one day and like I knew you were my son.

00:05:43

That's it.

00:05:50 Speaker 4

I don't think I've ever seen rocky and.

00:05:51 Speaker 2

Bullwinkle Ohh, you're missing out.

00:05:54

Ohh man.

00:05:57 Speaker 2

You're Canadian. The lead characters of Moose. How come you couldn't?

00:06:00 Speaker 2

Watch this like.

00:06:01 Speaker 3

Required viewing.

00:06:04 Speaker 4

Never seen it. I think there was a movie maybe that came out.

00:06:06 Speaker 4

When I was a.

00:06:07 Speaker 2

Kid, but yeah, there was a movie came out, it was really bad.

00:06:09 Speaker 1

Frostbite falls is not in Canada, it is in Minnesota. Thank.

00:06:13 Speaker 2

You very much. I know it is, however.

00:06:17 Speaker 2

It's got a moose.

00:06:18 Speaker 1

Yeah, well, then, Dudley, do right.

00:06:27

He's a mountie.

00:06:28 Speaker 1

Of course he's Canadian.

00:06:45

So how's the move?

00:06:45 Speaker 1

To motor I mean DC going.

00:06:48 Speaker 2

It's not yet.

00:06:52 Speaker 2

Still waiting on the Navy to catch up on all of my medical and admin stuff.

00:06:56 Speaker 2

Talk to my new boss. He's like hey, so.

00:07:00 Speaker 2

Here's the thing.

00:07:01 Speaker 2

Is even if you came up here, we wouldn't be sitting around.

00:07:03 Speaker 2

A board together.

00:07:03 Speaker 2

We'd be talking so, you know, we'll figure out when you need to be here. Cool.

00:07:10 Speaker 4

What's what's your new job, [Name Redacted]?

00:07:13

Yeah, I.

00:07:14 Speaker 2

Want to say I'm working for [Name Redacted]?

00:07:14 Speaker 4

What can?

00:07:16 Speaker 4

I say.

00:07:20 Speaker 1

And he's not.

00:07:20 Speaker 4

Where do I?

00:07:21 Speaker 4

Where do I know that name from? What do they what do they do?

00:07:24 Speaker 2

[Name Redacted] is a management consultancy company. They're the largest one in the world.

00:07:28 Speaker 1

It used to be [Name Redacted].

00:07:30 Speaker 2

What's that?

00:07:32 Speaker 1

They used to be [Name Redacted] before [Name Redacted].

00:07:35 Speaker 2

That the trait? Yep. And they've got a.

00:07:40 Speaker 2

Subsidiary that does work for the US government.

00:07:45 Speaker 2

Called [Name Redacted], and unfortunately, even though I had seven companies interested in me when COVID NIT.

00:07:45 Speaker 4

OK.

00:07:52 Speaker 2

This was the only one that didn't go. Hey, listen, we're going to put a hiring hold until.

00:07:59 Speaker 2

Until after COVID and the problem is I don't have a paycheck come July 1st, so I need a job.

00:08:07 Speaker 4

Yeah, fair enough. So.

00:08:08 Speaker 4

So you're with that. So you got that consultant life now, huh?

00:08:09 Speaker 5

I needed the money.

00:08:14 Speaker 2

Sort of, yeah.

00:08:17 Speaker 2

Basically, I'm just gonna be advising on a bunch of projects. I need to get smart on the practicalities of AI quickly. I'm not sure I should do.

00:08:26 Speaker 1

That first step is you go.

00:08:29 Speaker 1

Talk to [Name Redacted] and then that'll basically take care.

00:08:32 Speaker 1

Of all the other steps.

00:08:33 Speaker 5

OK.

00:08:39 Speaker 2

Trying to think if I have her e-mail somewhere.

00:08:43 Speaker 1

I can get it to you, otherwise I can give you her number and you can ping her on signal, which is.

00:08:49 Speaker 1

Generally, how she?

00:08:49 Speaker 2

Responds anyway. Yeah, if you don't mind doing that, that'd be great. I I could probably find my.

00:08:56 Speaker 2

My itinerary from the the event in November, but.

00:09:00 Speaker 2

Which, by the way, only horribly depressed if we don't have it this year.

00:09:06 Speaker 1

You and me both brother.

00:09:08 Speaker 4

Which event is this?

00:09:10 Speaker 1

One that you're probably.

00:09:11 Speaker 1

Gonna get invited to if I know [Name Redacted].

00:09:19 Speaker 4

It's like a AI conference is that?

00:09:21 Speaker 1

It's an invite only conference with all of the the Elder Dragon hackers from the beginnings of the Internet.

00:09:31 Speaker 4

That sounds ******* amazing.

00:09:34 Speaker 5

It is.

00:09:34 Speaker 2

It it is.

00:09:35 Speaker 2

Imagine the best conversation you've had in.

00:09:37 Speaker 2

Your life.

00:09:39 Speaker 2

And you're doing that.

00:09:40 Speaker 2

All weekend, every conversation for three.

00:09:41 Speaker 1

For, yeah, for three days.

00:09:43

Days. How do I?

00:09:45 Speaker 4

How do I live that lifestyle every day? Is there like?

00:09:48 Speaker 4

Secret there or?

00:09:50 Speaker 2

Yeah, it's there's so judicious that they actually rent out the entire resort, so that there are no outsiders during our event.

00:10:03 Speaker 4

Hey, [Name Redacted] and it's.

00:10:06 Speaker 4

You guys doing?

00:10:07 Speaker 6

Another day in Paradise, living the dream.

00:10:11 Speaker 2

Nightmares and dreams too.

00:10:12 Speaker 4

Right on.

00:10:39 Speaker 6

Having a little fun with the numbers today.

00:10:48 Speaker 1

I've been having fun with every possible way.

00:10:51 Speaker 1

You can misconfigured sushi.

00:10:52 Speaker 1

Enterprise Linux.

00:10:55 Speaker 6

Oh, that sounds almost infinite.

00:11:00 Speaker 1

It is when you work in compliance.

00:11:04 Speaker 1

There is a very limited range of things that can be considered correct in a very infinite range of things that can.

00:11:11 Speaker 1

Be considered incorrect? Yes.

00:11:18 Speaker 6

I just had to finish up a project where I had some fun doing.

00:11:22 Speaker 6

I I had to translate NIST documentation into English to submit questions to people. So in other words, are you implementing cryptography? Are you implementing cryptography according to this standard? Are you doing it according to this standard, and is it documented?

00:11:43 Speaker 6

Is your documentation reviewed on a periodic basis? How do you define periodic and? Then you have to do that for every class of information in there.

00:11:54 Speaker 1

Sounds like you you were playing with tips 143.

00:11:57 Speaker 6

Exactly. I'm sorry.

00:12:01 Speaker 6

And it was like I almost want to quote Father Mulcahy from mash the TV show.

00:12:12 Speaker 6

They you know, when it's our time to go to purgatory. Some of us can say no thanks. I've already done it.

00:12:29 Speaker 1

So what I'm working on for my day job is.

00:12:33 Speaker 1

So [Name Redacted] has a bunch of compliance configuration compliance auditing. Basically run the thing it tells you that this config file is correct. This one's not correct. This one has an extra line that are to.

00:12:43

Right.

00:12:46 Speaker 1

So you do that times.

00:12:48 Speaker 1

3400 depending on how what platform up to 1000 different unique checks in an audit.

00:12:57 Speaker 1

And then multiply that times basically.

00:13:00 Speaker 1

All the major server.

00:13:00 Speaker 1

Platforms. So Red Hat, 1-2, Susie, Debbie and then Windows.

00:13:07 Speaker 1

Server etcetera, right?

00:13:08 Speaker 1

And then you do it for all the the.

00:13:11 Speaker 1

SQL Server.

00:13:13 Speaker 1

And then you do it for.

00:13:16 Speaker 1

Maria DB, MySQL Enterprise and post grass and.

00:13:20 Speaker 1

Blah blah blah, blah. Well, it turns out.

00:13:23 Speaker 1

It's very hard to manage drift between those different audits, especially when there's a lot of shared content and it's very, very easy for things.

00:13:36 Speaker 1

To go.

00:13:38 Speaker 1

Wonky without you noticing.

00:13:41 Speaker 1

So I've been working on setting up.

00:13:44 Speaker 1

Ansible playbooks for all of these different platforms for different audits as a way.

00:13:50 Speaker 1

Of unit testing and configuration on it, so 3 playbooks per.

00:13:57 Speaker 1

Audit one for pass, one for fail and one for. Are you ******* kidding me? In terms of, you know, it's misconfigured the box as as badly.

00:14:05 Speaker 1

As you can.

00:14:09 Speaker 1

And then I'm running audits against it. So I've been doing.

00:14:11 Speaker 1

That got the.

00:14:12 Speaker 1

Bit between my teeth managed to break the box, the sushi box so badly that I had to.

00:14:20 Speaker 1

If I didn't have a snapshot in the VM, I would.

00:14:24 Speaker 1

Have had to reinstall.

00:14:28 Speaker 1

Well, turns out when you do things like change the permissions on Etsy password and Etsy shadow.

00:14:34 Speaker 1

The the system doesn't.

00:14:35 Speaker 1

Like it that much?

00:14:37 Speaker 6

No, you think?

00:14:39 Speaker 1

Yeah, well, I did it without realizing it cause it was.

00:14:42 Speaker 6

I'm beginning to think.

00:14:43 Speaker 6

I'm one of the last people left alive.

00:14:46 Speaker 6

Who was alive during the days when you had to have multiple machines? You know, no VMS, no snapshots. You had like 30 machines piled in your basement.

00:14:57 Speaker 1

No, I had for the longest time three machines tied together with synergy so that I could I could at least share a keyboard and mouse and clipboard.

00:15:08 Speaker 1

Yeah. EMS was the days.

00:15:13 Speaker 6

I just remember coming home from dumpster diving and you know, wow, another system to bring up.

00:15:23 Speaker 6

One thing I found though was uh.

00:15:27 Speaker 6

What were those things called? There were these awful.

00:15:30 Speaker 6

Horrible machines. They're called 3B's 3B twos or something like that.

00:15:36 Speaker 6

They they were the most clunky, unhappy machines in the world, but in the middle of the winter they made great space heaters.

00:15:45 Speaker 6

It was actually cheaper to run a couple of 3B's than to buy fuel oil.

00:15:51 Speaker 1

We had an old Irix, an SGI IRIX box, that we ran in the computer repair shop in college for that exact same reason.

00:16:18 Speaker 6

I can't find it. I thought it was called the 3B or something like that.

00:16:24 Speaker 6

I had one bit of fun today.

00:16:28 Speaker 6

I decided out of sheer boardroom and avoidance of cleaning the cat box. I would try to ship a bunch of my data out of the database into Excel.

00:16:40 Speaker 6

And I found something interesting.

00:16:44 Speaker 6

Take a look at that.

00:16:52 Speaker 1

OK. What are we looking at?

00:16:54 Speaker 6

Between the 30th of April and the 16th of May.

00:16:58 Speaker 6

Hashtag activity for Trump 2020 and WWG 1. WGA has kept pace with each other on a daily basis.

00:17:10 Speaker 5

That seems like it makes sense because.

00:17:13 Speaker 5

The Q and.

00:17:14 Speaker 5

On people would be in the same boat as the Trump people, right?

00:17:18 Speaker 6

Yeah, but to that level of of near identical levels of traffic.

00:17:22 Speaker 5

Interesting. Yeah, well, you know, you got one bot.

00:17:25 Speaker 5

Yeah, but.

00:17:28 Speaker 6

That's what I'm thinking. I mean, this is an indicator of either bot activity or they're, you know, pulling the trigger at the same time on on the you know the same.

00:17:37 Speaker 4

Thing the they got to talk to for this is [Name Redacted], [Name Redacted] and the this info channel I think.

00:17:45 Speaker 4

He's like our resident humanon expert. You might be able to.

00:17:49 Speaker 4

Give you some insight into that.

00:17:50

One of the.

00:17:51 Speaker 6

It's just the the numbers are the numbers are too close, too consistently to be an accident.

00:17:59 Speaker 3

Actually, someone was asking generally if.

00:18:01 Speaker 3

There was any bot IOC leads honest.

00:18:07 Speaker 3

One of the one of the leads on.

00:18:13 Speaker 6

Remember that is it sounds like you're underwater.

00:18:16 Speaker 3

Probably I'm on my stupid Bluetooth snake. I was just saying one of the one of the CIA leaders founders just put it at a a message out to everyone.

00:18:27 Speaker 3

I think following the general channel, maybe Disinfo asking if anyone.

00:18:32 Speaker 3

Observed any Iocs around bot activity bot networks.

00:18:37 Speaker 3

Like if anybody's looking.

00:18:38 Speaker 3

At broad Network, so I have a feeling you're probably seeing some signals someone else is seeing.

00:18:44

You might.

00:18:44 Speaker 3

Might look for that.

00:18:46 Speaker 6

I'm. I'm just at the point now where I've got the data collection going correctly and reasonably error free and I've gotten, you know, a couple of days solidly so.

00:19:02 Speaker 3

Wait for this, OK?

00:19:03 Speaker 6

I'm just getting. I'm just now getting to the point where I should be able to get some solid.

00:19:09 Speaker 6

Something you rather, whatever you folks would like. I've already had a few people request you know, specific queries and reports and stuff that's helped them out.

00:19:19 Speaker 5

Hey, [Name Redacted], would it be relatively easy to like pull that into Google Cloud platform or something like that where we could like automate some queries and start to like visualize the data?

00:19:30 Speaker 6

I want to say yes, but I don't know how just yet. What I've basically got is 2 mirrored DB databases.

00:19:40 Speaker 6

How to open those up safely and sanely?

00:19:45 Speaker 6

And get that to a point where people can submit their own request is something I'm working on.

00:19:52 Speaker 6

My initial thought was I would love to find a way to do it in an automated sense, but I've never done that before. Again, remember, I'm a sock analyst, AKA a sock monkey.

00:20:04 Speaker 6

So deep DBA automation is not my bag, so it's going to be slow.

00:20:09 Speaker 6

Going for a little bit.

00:20:13 Speaker 6

I'll pull apart an e-mail and I will shoot packets all day long and spit out reports, but I'm not a DBA.

00:20:22 Speaker 5

Cool. Well, what you're doing is awesome, so thank.

00:20:24 Speaker 5

You for that.

00:20:25 Speaker 6

The I I I I believe that I mean all I'm doing is exporting CSV's from the database. So as far as converting that to Google Sheets that shouldn't be a problem.

00:20:39 Speaker 1

So if you want a fun adventure off into Python land, there's a really cool library called Open Pie XL that basically will let you create an XLSX file from whatever input you want. I use it fairly frequently for both munging files and putting them into other formats, and also then.

00:20:59 Speaker 1

Creating excel files.

00:21:03 Speaker 6

Open π excel. Yep, I got.

00:21:05 Speaker 1

Yeah, open pyxel.

00:21:07 Speaker 4

It it's a good library.

00:21:11 Speaker 1

[Name Redacted], are you driving today?

00:21:15 Speaker 4

So we're going to finish off the training that as we started last week, we kind of when we got halfway through to talk about how the team can or should be structured and some of the rules we wanted to see. So today, we're actually going to dive into the AMMIT framework and I guess.

00:21:30 Speaker 4

OK.

00:21:35 Speaker 4

[Name Redacted], this is your baby. So you should.

00:21:38 Speaker 4

You should probably.

00:21:40 Speaker 4

Introduce it, I guess. Take.

00:21:42 Speaker 4

It from here.

00:21:44 Speaker 2

Yeah, yeah, I can do that. All right, so let me do this. All right. So basically, if you not really spend any time with the ammit framework, it's it's essentially the same kind of a format as miters attack framework. And that was done.

00:22:00 Speaker 2

Purposefully, when [Name Redacted] and I started this because I I also helped with the miter tech framework. So up at the very top line where you've got planning, preparation, execution, evaluation, those are those are execution phases. Those are the phases of the operation, the second line.

00:22:18 Speaker 2

Down is the kill chain. Now the definition of the kill chain is that you must complete a task in every link and if you fail to complete any link, the operation fails. So you can do all of the things and if you fail to develop networks then.

00:22:38 Speaker 2

You're you're.

00:22:39 Speaker 2

Influence campaign is just not going to work.

00:22:42 Speaker 2

And then the Gray boxes beneath the blue boxes are TTPS techniques, tactics, and procedures that can be used to complete that.

00:22:55 Speaker 2

That link in the chain. Now you can use some of these. You can use all of these. We don't think we necessarily have them all. Some of them may need to be redefined, but this serves as really as a

framework so that when I talk about center of gravity analysis, anybody in our group, regardless of the back ramp round should be able to go to Amit and go. OK.

00:23:15 Speaker 2

I understand what center of gravity analysis is and what you mean by when you say that and it it sounds trivial, but it it's not. It's actually quite.

00:23:24 Speaker 2

Quite complicated because we're all using slightly different languages. A trivial example of that is we talk about exploitation. If in in, you know, traditional infosec, you run an exploit at the beginning and then you conduct your operational objectives.

00:23:43 Speaker 2

Right when you're talking about human intelligence, your or influence campaigns, the exploitation is what happens after you've got the audience on your side. You exploit their views.

00:23:57 Speaker 2

And you exploit.

00:23:57 Speaker 2

Them to do your dirty work for.

00:24:00 Speaker 2

So you know, it's important to know, you know what it is that we're talking about, have everybody understand what the meaning of these?

00:24:06 Speaker 2

Terms are OK next slide.

00:24:15 Speaker 2

Types of accounts, lots of types of accounts, but very roughly they can be binned in this way. Bots bots are relatively stupid. They're getting better, but it's still not terribly hard to find bots. Bots don't typically generate content. They're usually used to amplify messages from a couple of the small accounts that put out the initial.

00:24:35 Speaker 2

Content parities parity counts are not supposed to be.

00:24:43 Speaker 2

Mistaken for the real accounts, but oftentimes they they are. They're meant to be funny. They're meant to make fun of the of the actual entity, like the.

00:24:56 Speaker 2

There were a bunch of.

00:24:59 Speaker 2

Accounts on Twitter that were like, you know, the underground White House staff, right. Nobody would mistake that for the real White House staff.

00:25:07 Speaker 2

But it made fun.

00:25:08 Speaker 2

Of the real White House staff, so that kind of things then you've got impersonation accounts. Those are meant to be mistaken for real accounts.

00:25:18 Speaker 2

And so they've got to be close enough to the real personality that it can be a thing. This is a fairly common tactic, as you all know, where you know, there's a reason that, you know, Donald Trump's thing is the real Donald Trump. Because if you look for Donald Trump on Twitter, there's a bunch of them. Every one of them more intelligent than the.

00:25:36 Speaker 2

Thing the next one, the the wolf in sheep's clothing. That's when you try to infiltrate a group and then you what you do is you espouse their beliefs, and once you're in that group, what you can do is you can actually steer the group to do things. You saw this a lot with the.

00:25:58 Speaker 2

Far right wing, you know, white power, hate groups and the black lives Matters in 2016, where they were obviously infiltrated, and they were convinced to hold events at the exact same time at the exact same place. Several times. That doesn't happen on accident.

00:26:15 Speaker 2

The trust. No one is a deep cover account. These are getting harder and harder to create. These are fake people, right? They're personas. They have to be backstopped. And it's getting harder to create them because it's very difficult to go in there.

00:26:28 Speaker 2

And create a.

00:26:30 Speaker 2

A history, right? If you see somebody.

00:26:32 Speaker 2

Posting something on Facebook.

00:26:34 Speaker 2

And that account's only been around.

00:26:36 Speaker 2

For like 3 weeks.

00:26:37 Speaker 2

It looks kind of suspect. Most people been on Facebook for a couple of years.

00:26:41 Speaker 2

Right. And then the last one is the hijack that the chess board is the hijack and that's when you you actually hack the legitimate account and post as if you're them. So the best example of this was October 2013, somebody hijacked The Associated Press.

00:27:01 Speaker 2

Count and put out a tweet saying that there had been a bombing at the White House and that President Obama had been injured and it actually caused the stock market to drop and it set off the the tripwires. The circuit Breakers. Next slide.

00:27:18 Speaker 2

So using those types of accounts, what are the strategies [Name redacted] gave us? Four of these? I added a fifth one, so [Name Redacted] gave us distort, dismissed, distract, dismay, and to that I added divide. So distort is when you take the narrative.

00:27:36 Speaker 2

And you just twist it ever so slightly to come up with a different conclusion. So the Russians didn't invade Crimea, they were liberating ethnic Russians, right. So whether or not which of those you believe is probably going to be very much based on where you are in the world and how you grew up.

00:27:54 Speaker 2

Dismiss is typical of the Chinese is their favorite tactic. Every time they accuse them of something they say no, no, no, that's ridiculous. You're making, you know, outlandish accusations, by the way. We're always, you know, the victims of American imperialism, hostility hacking.

00:28:10 Speaker 2

You name it.

00:28:12 Speaker 2

Distract is when you take an existing.

00:28:16 Speaker 2

Creative that you don't like and instead of distorting it or dismissing it, you try to create a different narrative about that event. So the MH 17 being shut down by missiles provided by Russia. You know the

Russians tried to distract people by going why is there commercial airliner flying over an active war zone? You know who's who's responsible for this?

00:28:36 Speaker 2

Dismays the ad hominem. Those are personal attacks, and just by responding to them, what you've done is you've acknowledged it and therefore made it seem plausible, right? So the, you know, the pizza gate comment pizza, sex dot.

00:28:50 Speaker 2

Engine. You know, in the basement thing there, there's no way to reply to that without letting it some credence. If it's so ridiculous, you wouldn't even respond. And then the last one is divide. This was the one used in 2016. So again this is, you know, the Russians hopping into and and bifurcating the US populace.

00:29:10 Speaker 2

Right into two groups and getting them warring with each other so that they're angry at each other, not looking at the big picture. And the Russians are really, really good at that.

00:29:19 Speaker 2

Next slide.

00:29:26 Speaker 2

So the stage based models are useful because it allows you to kind of look at things at the strategic, the operational and the tactical view and and that's why we've got the multiple layers in the Amit, we're pretty sure we have the top two layers correct.

00:29:42 Speaker 2

The lower layers, we don't know that we have them correct. We we initially took a look at a bunch of well known misinformation campaigns. We try to bid them, but we may need to.

00:29:52 Speaker 2

Adjust them. It's just helpful depending on who you're talking to that you know which layer you should be at, and that allows you to.

00:30:03 Speaker 2

Then put it into Miss [Name Redacted] done a fantastic job of of inserting the Emmett framework into MISP and our other tools so that we can share the information. Next slide.

00:30:19 Speaker 2

So the attack framework, I think everybody's familiar with the attack framework. This was a a framework that mitre developed for describing cybersecurity incidents and the reason that they did it is back in the early 22 thousand, 2000.

00:30:38 Speaker 2

8910.

00:30:41 Speaker 2

Lots of people were talking about cyber, but when a lawyer was saying one word, it meant something completely different than when a stock analyst said that same thing. And so this was an attempt to get a a lingua franca and it set up in much the same way as Amit. So we when we built Amit, we we extended attack to cover not only.

00:31:01 Speaker 2

Cyber incidents but influence and misinformation incidents. Next slide.

00:31:10 Speaker 2

So as I kind of mentioned we we populated Amit as we were developing it based upon campaigns, Internet Research Agency 2016 elections, different incidents like the Columbia chemical plant explosion and then failed.

00:31:27 Speaker 2

Attempts like the Russian influence attempt to influence the French campaigns. We started out by taking a look at roughly 106.

00:31:36 Speaker 2

50 different incidents in campaigns and then we were able to kind of distill those down based upon unique TTP's to make sure that we had the best coverage possible. Next slide.

00:31:55 Speaker 2

So this is, you know, an example of the data sheet that we used. So in this case, the Internet research agency, you know, the actor was probably the IRA. We had a time frame. We were able to kind of discern a goal or or make an educated guess of the.

00:32:11 Speaker 2

We are able to pull out artifacts related to text, so forth and and that's why you see it laid out in the way that we've got it laid out now in miss next slide.

00:32:25 Speaker 2

As you get these different incidents and you see these different artifacts, it's going to feed in the techniques list. And so again, we don't have all of the techniques. We don't claim to have all of the techniques, but everything that we've seen right now, we're able to kind of bend in one of the.

00:32:41 Speaker 2

TP's that we've got.

00:32:43 Speaker 2

As TTPS change because they will.

00:32:46 Speaker 2

We'll have to go in there and make sure that our bins are still valid or if we need to either split bins or add additional bins so that we can get the information that we need. Next slide.

00:33:03 Speaker 2

So if you've, if you've seen the pyramid.

00:33:07 Speaker 2

You know, up at the top is campaigns and down at the bottom is artifacts. If you've not seen that, I think it may be in a couple of slides. If you're conducting a campaign, you actually start at the top of the pyramid, you know what you need to do. You've got your commanders intent.

00:33:27 Speaker 2

And so you can, uh.

00:33:31 Speaker 2

You can build your objectives from there. You can build your narratives from there and you can build the artifacts that support their narratives that support the objectives that support the campaign. And just like you know, a real pyramid. If you start at the top, getting to the bottom is fairly effortless, right? You you already know what the board looks like, and you can just, you know.

00:33:51 Speaker 2

Scoot on down without much effort the problem.

00:33:53 Speaker 2

That we've got.

00:33:55 Speaker 2

As as defenders trying to counter this is, we're starting at the bottom right. We're starting at the tactical level as opposed to the strategic level started by the the the guys and gals that made the influence campaign. And so when every time we get a piece of data, we've got to figure out you know, is this an artifact, right, is this hashtag an artifact?

00:34:15 Speaker 2

This is a start of a trend or topic or a new platform activity. If it is, we can go up and go. Is this part of existing narrative or is this part of a new narrative? And then once we decide that we can go up and decide, OK, well, what objectives to serve and who.

00:34:30 Speaker 2

Might be responsible for.

00:34:32 Speaker 2

But climbing up makes takes time, right, and takes a lot of effort because you know, if you see a hashtag once, it may not mean anything. You may see a hashtag a lot 1 day, and it may just be a blip in the radar. So really doing the analysis and figuring out how to connect all those dots or if the dots even should be connected. That's the hard part.

00:34:51 Speaker 2

Next slide.

00:34:57 Speaker 2

Again, this is just the Amet framework in in table format, so the planning stages, you've got strategic planning and objective planning preparation. Those are the different links in the chain execution and then evaluation. The only one that we've got that is kind of an optional.

00:35:14 Speaker 2

Link in that chain is micro targeting. Depending on your objective, you may or may not have to micro target.

00:35:22 Speaker 2

Next slide.

00:35:25 Speaker 2

Roger, do you want to talk about this or do you want me to?

00:35:30 Speaker 4

Go ahead. Go ahead. Go for it.

00:35:33 Speaker 2

OK, so this.

00:35:34 Speaker 2

Is the. This is the Amet framework.

00:35:40 Speaker 2

That's been instituted and missed. And so you can you can see at the strategic planning we've got those five days dismissed, distort, distract, dismay, divide and competing narratives and facilitating state propaganda. And so as you go through and you you build the Galaxy right and you build the artifacts, you start.

00:36:00 Speaker 2

What you'll start seeing is all of the little pieces of evidence that we've gotten, all of the artifacts that support that conclusion for this campaign, and you're probably going to start out by just seeing, you know, one or two small things. You're you're very rarely going to get the whole chain at once.

00:36:20 Speaker 2

But you will overtime and it's just a matter.

00:36:24 Speaker 2

Of you know, taking the artifacts and figuring out, you know, does this link into something we're already aware of? There's this new and you make an initial gut call later on, you may figure out that, hey, listen, these two narratives are part of the same campaign, and you can merge them. But, but you may not. You may not know when you start out next slide.

00:36:48 Speaker 2

So we've got these TTPS where we're at now is how do we counter it, right? So everybody wants to get to doing something about it. The problem here is it's a minefield, right? And the reason it's a minefield is most people, including most of us, have never really sat down.

00:37:09 Speaker 2

And consider.

00:37:11 Speaker 2

How we might counter a narrative right? Usually it's a it it. It's kind of like when we started out with Infosec. It's well, we wait for an incident and we respond well. It's you can't really do that, right? It doesn't work in Infosec and it doesn't work at influence campaigns and misinformation. So.

00:37:30 Speaker 2

1st, we can't talk about things that we would do to counter it after an incident, and then it's a matter of not just what can the Infosec people do, but what can the policy people do? What can the journalists do? What can we and the lawyers let us do? The problem is particularly for the government.

00:37:47 Speaker 2

And I'll speak specifically about the US government.

00:37:50 Speaker 2

Cause I'm I'm.

00:37:50 Speaker 2

Not entirely sure how Canada has it.

00:37:52 Speaker 2

Set up is the people that have the capability don't have the legal authority.

00:37:57 Speaker 2

Right. And so the people that have the capability and expertise to do this is the US Department of Defense, but the US Department of Defense is expressly forbidden by presidential directive and by law from operating against U.S. citizens. Right. And so.

00:38:19 Speaker 2

It's a kind of 1/3 rail and so nobody in the US military wants to touch this and counter misinformation in the United States. So then you go well it it should be the Department of Homeland Security that would do this. But they have neither expertise nor do they have the capability to do it right. They don't have the.

00:38:37 Speaker 2

People to do it.

00:38:39 Speaker 2

The people that do it overseas are typically.

00:38:43 Speaker 2

The CIA and the NSA and the Department of Defense, but again, I've already talked about that Intel collection agencies are not legally allowed to do those things inside the United States. And even with the best of intentions, Americans have a healthy distrust of their government. And it just wouldn't look good. So the people it's actually sitting with right now.

00:39:04 Speaker 2

Is the Department of State and the Department of State now has a new cell called the GAC. The Global Engagement Center, and they're supposed to be doing it now. They're essentially brand new. They're just getting something like.

00:39:22 Speaker 2

$250 million next fiscal year. They're just ramping up, frankly, they're not very capable right now.

00:39:29 Speaker 2

But we need to help them out by deciding, you know, what kind of things can we do proactively? Yes, education is great for the kids that are in school now, but what would you what do we do with John and Jane Q. Citizen that actually, you know, watch Fox News and believe pandemic what do we do with those guys? How do we educate them so they don't fall for the next thing.

00:39:51 Speaker 2

Next slide.

00:39:53 Speaker 4

That's the last slide that's that's it.

00:39:55 Speaker 6

All right, so.

00:39:56 Speaker 2

I think that's it. Let's [Name Redacted] or [Name Redacted] you.

00:39:58 Speaker 2

Guys want to jump in and add something I forgot.

00:40:04 Speaker 4

So one. Yeah, I think you covered everything. And the one thing that I'd like to go back to is the idea of. So you know, that covers what the AMMIT framework is, what you guys built, why you built it, what we're trying to.

00:40:18 Speaker 4

Do, but maybe we should look at practical application, right? What? What? We're sitting in slack we have.

00:40:24 Speaker 4

This information incident you.

00:40:26 Speaker 4

Know, we suspect is interesting.

00:40:29 Speaker 4

How can we start modeling that to the AMET framework? How do we start applying the techniques? You know, what should we look for? Does it make sense to start tactic by tactic? Do we look at techniques and then look for like parallel capability or tangential capabilities or whatever? So that might be maybe something to get into and also we can talk about how we.

00:40:49 Speaker 4

To translate that into the tools in this or the navigator.

00:40:56 Speaker 2

And this thing I mean, you know, in the military they call this operational art and the reason they call it operational art is because it sure should not a science. A lot of this is based upon experience and intuition. So when you see that artifact and you go, OK, somebody's trying to do something here.

00:41:13 Speaker 2

Right, the analyst needs to sit there and try to figure out just like we do in Infosec, you know, what is it that they're attempting to accomplish here? How are they doing it? What is the and you know, who is the intended audience? What is the intended effect?

00:41:30 Speaker 2

And a lot of times it's it's really just a best guess.

00:41:36 Speaker 4

What are your thoughts on what are your thoughts on on working through this? So you mentioned that, excuse me that this is a kill chain and you know we have a a linear progression. Each tactic is required, but obviously this loops back right? Like we can do things in parallel and we could go and develop.

00:41:56 Speaker 4

Content prior to developing a network or go back and redevelop content. So given a starting point, I mean, what are your thoughts on like?

00:42:06 Speaker 4

What to trace back to like? Sorry, this is word salad. Let me get my question straight. OK, given a starting point of.

00:42:16 Speaker 4

Of of content you know we see like memes come in or a news article or something. Should we trace that?

00:42:25 Speaker 4

That can try and identify people first networks first. You know channel selection importance. Are we looking for, you know, evidence of Twitter bots? Like, any thoughts on?

00:42:39 Speaker 4

I don't know four steps there or.

00:42:42 Speaker 2

Yeah, you know, unfortunately my answer is going to be wholly unsatisfying, right? It it's, it's, it's really going to have to be a best guess, right. And now some things.

00:42:46 Speaker 4

OK.

00:42:50 Speaker 2

Are obvious, right?

00:42:52 Speaker 2

I mean, if you see a queue and on tag then you I mean you know who it is, right? You know who they.

00:42:56 Speaker 2

Is a lot of times by looking at the message itself, it's very transparent.

00:43:03 Speaker 2

Current who the target audience is, right. Sometimes it's not, sometimes, sometimes it's one of those things that you're like, oh, this is interesting. OK, well, it's just a joke, and you don't realize it's actually hooked into a narrative and an influence campaign until much, much later. And then.

00:43:19 Speaker 2

You have to go back and look at it.

00:43:24 Speaker 5

OK, I was going to ask to what extent have you operationalized this as a team before? Like if I'm trying to collaborate with you and [Name Redacted] on this, like, how do we do, how, how would that actually kind of come to fruition?

00:43:24 Speaker 2

Go ahead.

00:43:39 Speaker 2

Roger, do you want to?

00:43:40 Speaker 4

Take that one. Yeah. I was like that. So the big book documents how we're going to kick off an incident. Right. Opening up events in Minsk or creating notes in the in the README. The first steps, I think part of the most important steps that we can.

00:43:59 Speaker 4

We can take initially is to start mapping out the techniques that we find to the navigator or to the galaxies in this to get a sense of what the capabilities are that are being expressed. And I think that can kind of.

00:44:11 Speaker 4

Guide our reasoning into whether or not it's an interesting operation. What I mean is, many techniques will be common and we'll see the same things over and over again like generating memes right or creating sock puppets, but there are some that I expect and I could be wrong.

00:44:32 Speaker 4

Require a lot more organization and forethought, such as organizing merchandise or going physical with rallies and coordinating.

00:44:42 Speaker 4

As we saw in 2016 to groups that would potentially come into conflict to occupy the same space at the same time, that's probably not a trivial thing to do, right, so.

00:44:56 Speaker 4

What I'm saying is, as a first step, we just need to get kind of a a lay of the land for for what the capabilities are that we're observing and.

00:45:05 Speaker 4

I don't know if.

00:45:05 Speaker 4

There's, I don't know if there's a a procedural way to do that other than to just start sifting through the information and mapping it here onto this matrix and tagging it into.

00:45:16 Speaker 4

Into MySQL.

00:45:19 Speaker 4

Does that answer your question?

00:45:22 Speaker 5

I think so and then.

00:45:24 Speaker 5

I guess a quick follow up.

00:45:25 Speaker 5

Would be.

00:45:26 Speaker 5

Is there a place where these different pieces are kind of like spelled out and defined? So we're on the same page about what each of these?

00:45:33 Speaker 4

Means. Yeah. So yeah, you can now. So this is the, this is the navigator you can.

00:45:34 Speaker 2

One question.

00:45:43 Speaker 4

Right click and view technique and this will dump you in the GitHub page with the definition.

00:45:49 Speaker 5

OK.

00:45:50 Speaker 4

But this information is is also in in mist and I don't.

00:45:57 Speaker 4

I don't have it here, but in miss there's just like a little.

00:46:01 Speaker 4

Plus icon drop down icon besides the Galaxy definition and if you click on that it'll tell you the it'll give you this same text definition. I would. I would recommend like as an exercise to just read through the entire list. You know just to get an idea for what's there. Some of some of the names might not be.

00:46:21 Speaker 4

For obvious what's actually intended, you know, or the definitions, little nuance, a little more nuanced than.

00:46:27 Speaker 4

The names. So that's it.

00:46:30 Speaker 5

Awesome. Thanks.

00:46:42 Speaker 4

Yeah. So I think this meeting.

00:46:46 Speaker 4

'S about to run out of time maybe.

00:46:48 Speaker 4

Like 4 minutes 5 minutes.

00:46:51 Speaker 1

No, you've got the unlimited account with.

00:46:53 Speaker 1

Me so 24 hours but.

00:46:54 Speaker 4

OK, cool. So the the actual culture measures follow up. That's gonna be a second training I guess we talked about what Amit is.

00:46:56 Speaker 1

Please don't run that long.

00:47:08 Speaker 4

What the techniques are?

00:47:12 Speaker 4

How we can start modeling this technique and an?

00:47:15 Speaker 4

Incident in this.

00:47:17 Speaker 4

Is there anything else, [Name Redacted], that that we need to talk about here?

00:47:22 Speaker 2

No, I think the biggest point is just to to get familiar with the book, get familiar with Amit and then when?

00:47:29 Speaker 2

You want access to the tools.

00:47:31 Speaker 2

[Name Redacted] can help you get.

00:47:32 Speaker 2

Access to the tools stuff.

00:47:33 Speaker 4

Oh, actually, yeah, actually, the the one thing I wanted to mention astray and I and I think we talked about.

00:47:35 Speaker 2

Go ahead.

00:47:41 Speaker 4

As well, we actually as a group, you know as teams or whatever we need to take existing threat Intel reports, you know like from graphic card Fr Lab or whoever and read through those as an exercise and and map out their findings into the into the framework. I did that with.

00:48:01 Speaker 4

Some graph.

00:48:03 Speaker 4

Reports previously just to get a feel for Emmett, and it was actually a really good way to internalize, you know, exactly.

00:48:11 Speaker 4

What? What these?

00:48:11 Speaker 4

Things mean and.

00:48:13 Speaker 4

You know when it's appropriate to use them, and I think if we do that a few times with the, with the folks in here, you'd get a really, you know, solid understanding.

00:48:22 Speaker 4

Rather than just like looking at a.

00:48:24 Speaker 4

Matrix, so I will organize that and then.

00:48:29 Speaker 4

Once that's once that's completed, you know we'll have the finished product. We can hand that off to other folks. You know, so kind of work through it as an exercise and we don't necessarily need to be there.

00:48:56 Speaker 4

So yeah, that's all I've got.

00:49:01 Speaker 1

Any other questions? Otherwise I'm going.

00:49:03 Speaker 1

To open up the happy hour zoom call.

00:49:15 Speaker 1

Going once.

00:49:19 Speaker 1

Going twice.

00:49:21 Speaker 1

All right. I will put the link for happy hour in Slack and I will see you all shortly.

00:49:28 Speaker 1

Thank you very much, [Name redacted].

00:49:28 Speaker 1

And [Name Redacted], thank you.

00:49:29 Speaker 3

OK.