# Chapter 8 Incident Response



## TL;DR Incident Response

Match your response to the time that you can make a difference in, the team and resources you have available, and the effects that you can reasonably achieve. It's okay to say 'no' to response.  If you respond, name the incident, decide which questions you're answering, tell the team that you're responding and sort out where response inputs and outputs are going.

## Disinformation Threat Intelligence

On a large scale, we see what we do as being part of threat intelligence: the prediction and analysis of recent, current and future threats. To do that, we use:

- **Intelligence analysis**: determine what's going on, who's involved, and what our best guesses are about the current and future situation picture.
- **OSINT**: using public data, determine what we can tell responders, in time for them to act
- **Data science**: support the intelligence analysis and OSINT by finding patterns and information in the data we have available, and help with the "three Vs": the triple problem of data coming in too quickly, at too great a volume, or in too wide a set of formats for the team of people we have available to analyze in the time we have to respond.

# Incident Response Considerations

If you're creating a response team, or a new type of response within a team, there are a bunch of axes to think about. How we do this work is evolving rapidly. Another area that also rapidly evolved recently is data science. We've borrowed liberally from data science, intelligence analysis and OSINT practice to help us make sense of this.

## Response Timescale

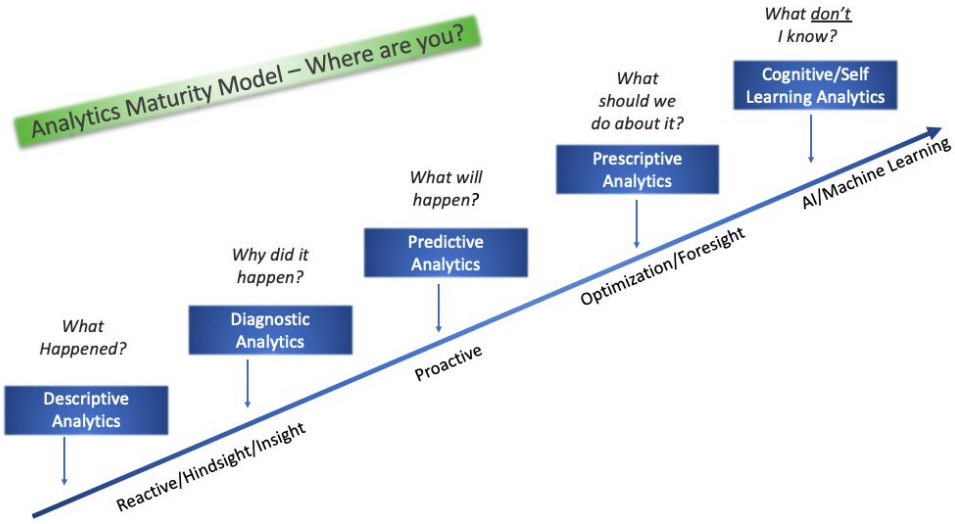
Simply put, how long do you have before your analysis and actions don't make a difference? We've divided both data science and disinformation in terms of response times:

- Strategic - years/months/weeks. Issue focussed (e.g. in-depth investigations, long-form journalism). Good places to look for this type of work include Stanford Internet Observatory, UWashington, Shorenstein Center, Bellingcat, Dfrlab, social media platforms.
- Operational - days/weeks. Project focussed. Examples include data scientists embedded in dev teams, working to answer questions/ build algorithms within software dev cycles. Usually running hypotheses to support things like behaviour-driven and hypothesis-driven development, and lean enterprise (pruning value trees etc). Good places to look include the AI/ML-based disinformation data and tool companies.
- Tactical - hours/days. Incident focussed. Includes data journalists. Good places to look include New York Times, CTI League team, some of MLSEC, some of the crisis-mappers.

Different teams do different things. Some teams are large and fast; others small, slow and deliberate. They're all part of a much-needed response. Interestingly, many of the strategic teams are now becoming more tactical in their response, as their baseline data, tools and connections improve. The TL;DR for this axis is that if you only have hours, all you care about

is stopping the flood; if you have months, you can get into the details of attribution, geopolitics and motives.

## Level of Engagement




Analytics maturity model (aka the Data Science Ladder)]

Data science is sometimes described in terms of the data science ladder (above). It describes the types of work done by teams, from investigating what has happened in the past (e.g. classic statistics), to predicting what might happen next, to suggesting moves and countermoves in an interactive environment. Disinformation response is moving towards the right of this ladder now, hovering somewhere around prescriptive analytics (e.g. groups are starting to both analyse and respond, but not engage in game-like interactions yet). Which part of the ladder will the data part of your response be on?

## Product types

We could also divide data scientists by the things that they care about:

- Academics - long deadlines, care about papers and reputation
- Academics working on techniques - UIndiana
- Academics analysing actors and issues - DFRlab, strategic
- Government agencies / military - strategic
- Commercial interests

What is your team, and the teams around it, really trying to do? What are the objects that are most important to it (artefacts, narratives, actors, intents?) - this will shape what you produce and for whom.

### Resource Constraints

Although data science is used to make sense of the large data flows in social media, much disinformation response work is still done by hand and is very similar to classic OSINT.

Just because you want to do it doesn't mean you can (or can yet). Do you have the resources for large-scale data analysis?  Is your team recovered enough from its previous deployment(s) to engage in this one?

## Incident Workflow

The main workflow in the disinformation team is tracking an incident.

A new rumour has started online. You've seen it yourself, someone has sent you an example of it, you've seen another group tracking it - there are a bunch of ways to spot something new happening. The steps that happen next are:

1. Decide whether to start an incident
2. Add incident to logs
3. Alert the team
4. Create places to put incident outputs
5. Build a situation picture
6. Share the situation picture
7. Take or spark action

### Make a Go/No-go Decision

An incident needs to be within the team's scope, and large enough to be worth expending team effort on.

Before you start, do a quick check that it's a rumour. One sighting doesn't make an incident. 15 copies of the same message on Twitter, or 3 friends sending you the same strange DM, and you're probably onto something.

When we see an alert, we have some questions:

- Is this an incident, e.g. is it a large coordinated disinformation incident, or an isolated piece / few pieces of disinformation?

- Is this disinformation suitable for processing by the disinformation team (e.g. 419 scams might be better handled by the Phishing team, but might also contain information about incidents that we should check out too)?
- Is this disinformation already being handled by platform teams or other specialist teams (we might want to check in with them just in case, for instance referring to healthcare groups ior law enforcement, or issuing a takedown request because of a finding)?
- Is this incident something that we should track?

“Is this incident something that we should track?”, e.g. how do we choose which incidents to track?

- We don’t track incidents for fun or interest. We track the ones that we have a reasonable chance of doing something useful about - whether that’s raising the alarm to groups or organisations that can respond to the incident, asking them to take specific actions (like taking down a disinformation account or site), or taking actions ourselves (like amplifying counternarratives).
- We also track and counter incidents that we believe give us the best chance of a positive effect, and in the Covid19 deployment, ideally one that impacts health.

Tracked cases can also include persistent threats - groups, narratives, artefacts etc that are likely to appear in future incidents.

## Triage questions

The first questions are about whether to start a response.  Since questions usually create new questions, this will also feed into your list of things to prioritise, and/or investigate.

- Is this potentially doing harm?
    - What effects might this have?
    - Is it large? Coordinated? Targetted (to demographics etc)?
- Is this disinformation
    - Is the content false (e.g. misinformation?)
    - Is it e.g. phishing rather than disinformation?
    - Does it include fake groups, fake profiles, fake amplification etc
- Is our team the best one to respond to this?
    - Is this in our area (e.g. CTI = currently working on Covid19 / medically-related?)
    - Is someone else already tracking and responding to this?
    - Do we have the resources to respond?

There are several follow-on questions to these, e.g.

- Is this isn't an incident, is it something that we should handle in a different way? e.g.
    - investigate as part of our monitoring work

    - monitor periodically in case it becomes an incident
- If we're not the right team, and nobody else is tracking this, should we:
    - ignore it
    - put out an alert in the hope that another team might pick it up
    - work to find a more suitable team for it

## Add incident to logs

Give the incident a memorable name. This helps.  Add the incident to whichever system the team is using to track incidents.  This gives the rest of the team, who are often on different time schedules, a heads-up that this is an active incident.

## Alert the Team

- Put a message in slack, with the artifact you found and a short description.
    - Start with “NEW RUMOR” so we will be able to track them
    - Any supporting information or links (under that rumor) should be posted in a thread off that initial NEW RUMOR post
    - This will make documenting and adding objects and observables to the incident and analysis log easier to track, and also keep everything a little more tidy

At this point, might also send out flash alerts to connected teams too.

## Create Places to Put Outputs

- Create a folder in the \[googledrive INCIDENTS folder\] for notes and anything that won’t fit into the DKAN
- Start adding data to the DKAN

When you create a disinformation incident in HIVE:

- Create a new case. Use case template “Influence Operation Incident”.
- Name the incident (use this name in all the tools)
- Create an event in MISP for the incident
- List the risks and potential real-world consequences from this incident
- List any time bounds on the incident, e.g. are there events that it’s gearing towards etc
- List any geographical or demographic targets in this incident
- Create a DKAN directory for the incident

MISP list for starting an incident

- List actors and other objects that are important in this incident - we're using a combination of STIX and DFRlab's Disinformation Dichotomies standard for this. Add these to the Clean MISP
- List the tactics and techniques that are being used in the incident - we're using AMITT for this (the version that comes as standard in MISP). Add these to the MISP event.

DKAN holds data we don't want to lose, and data that's raw and large: it's the in-tray

MISP hold objects of interest and the relationships between them, so we can quickly look up things we've seen before etc

## Build Situation Picture

Look for related artefacts, accounts, urls, narratives etc

Data we build up in MISP

- Incidents
- Narratives
- Actors
- Urls

## Take or Spark Action

- Investigate ways to close down the rumor / repeater sites etc.
- Report on the rumor
    - Add an incident to the MISP instance for this rumor
    - The incident must include some relevant observables such as a Tweet, social media username or URL.
- Write and send notes/reports to the people who can respond
- Close down the rumor and move onto the next one (there's always a next one)

## Help with a disinformation incident

- The master document for what we're doing on incidents is the [incidents spreadsheet]. Look at the status column - the priority is live incidents, then monitor long-term, then "keep an eye on it" (the potential 'zombie' incidents that are probably dead but might restart)
- Check back in the slack channel, and in the incident README in the [googledrive INCIDENTS folder] to see what's been done with this incident recently. As we get things together, we'll probably have incident-specific tasks in the github issues list, but we're still working on that.

- Find articles and artifacts, investigate the ones we have, put results into the slack channel for harvesting by the bots, and/or discussion with the team.
- If you spot something significant (new objects tied to the incident etc, new things of interest), update the incident README.

# Organising an Incident Response

Documenting analysis:

- We have DKAN and MISP, but also useful to have a google folder for each incident for other things that don't fit into those, like research notes
- Classifications: if it's openly available online, then it's okay to put through e.g. Tableau; if it's come though internal routes (e.g. SMS), then keep it off public internet (don't share).
- looking for related artifacts, urls, narratives etc

Who we communicate to:

- Report when something significant happens - e.g. see this main effort for this new line
- Report on time period… if big, a daily report; if smaller a weekly report
- No report goes out without at least 2 people beyond the editor going over it
- End users are also watching the MISP

Who makes decisions:

- Depends on decisions
- Need a board - vote via slack; person calling for vote does @channel to board, or emails them
- Who can add an incident? Anyone can start an incident.
- Who can release a report -
- Who can talk to customer/ victim? Needs to be agreed on

## Managing an incident response

An individual can track an incident on their own - open up some notebooks, fire up the coffeemakers and mainline chocolate for a couple of days. That's - not sustainable over time and large numbers of incidents, any more than it is for other infosec incidents.

The short instructions for managing a response are in the \[team readme\]. This is some of the thinking around them:

We haven't worked out exactly how to fit cognitive security / disinformation response into a SOC yet, but here's where we are at the moment on starting an incident:

- Incidents need names. Yes, yes, I know that's a slippery slope that ends up in a cute mascot and a dedicated website, but a name makes it easy to quickly identify what you're working on, find the right folder to put things into etc.
    - Action: Make up a name: make it short but descriptive - you're going to be typing it a lot, but you also want to remember what it was about a week later.
- The team needs to know you started an incident - both the team who are around at the time (and can help look for artifacts, add their specialist skills etc), team members who are coming in looking for things to do later, and leads who are trying to balance the load on the team overall. Best way to do this is to add a note to the team chat and an entry in the team log.
    - Action: add a note to the team slack channel, naming the incident and asking for help with it (if needed). If you have a starting artefact, add that too. Adding the word "NEW" will make it easier to find by people looking in on the channel later.
    - Action: add an entry in the team log, saying you're starting an incident response. At the moment, this is the incidents spreadsheet - this is likely to shift to adding a case to an incident tracking tool like TheHive.
- You, and the team, are going to start producing notes and artifacts as you track through the incident. Create a place to put them, that's accessible to the team
    - Action: create a space to put images, artifacts etc in. At the moment, that's creating a folder for the incident under the INCIDENTS googlefolder - this is likely to shift to directly uploading to a tool like TheHive or MISP.
    - Action: create a notes log for the incident. At the moment, that's a README file in the incident googlefolder - this is likely to stay the same for the moment. In the log, write a short description of the incident, and how you started tracking it (e.g. what the first artefact(s) you saw were.

Here's where we are on managing investigating the incident:

- You, and the team, are going to investigate the incident
    - Action: Look for related artefacts, accounts, urls, narratives etc
    - Action: add artefacts to the space you set up for collecting images, artefacts etc. You'll find it helpful if you number the images, because they're difficult to reference otherwise (aka "the yellow poster again" isn't as specific as "image001_yellowposter")
    - Action: keep the flow of investigation moving - keep a list of actions related to the artefacts, and/or direct the team to areas that need further research
- You'll also need to translate that into an incident description that can go out as an alert to other teams, and be used to look for potential counters
    - Action: add incident to alert tools. We're using MISP here, so adding a MISP object for the incident, and attaching the objects important to it is appropriate here.

    - Action: map artefacts seen to tactics and techniques. MISP includes AMITT - you can use the ATT&CK navigator to click on all the tactics and techniques you can see in this incident.
    - Action: Investigate ways to close down the rumor / repeater sites etc. We're working on tools for this too, but for now it's discuss this with the team, and check the lists below.
- Oh, and yes, you get to be scribe for the team too, making sure you keep a record of the investigation:
    - Action: keep the incident log updated with any significant findings, notes, things to do etc.

And here's where we are on managing responding to the incident:

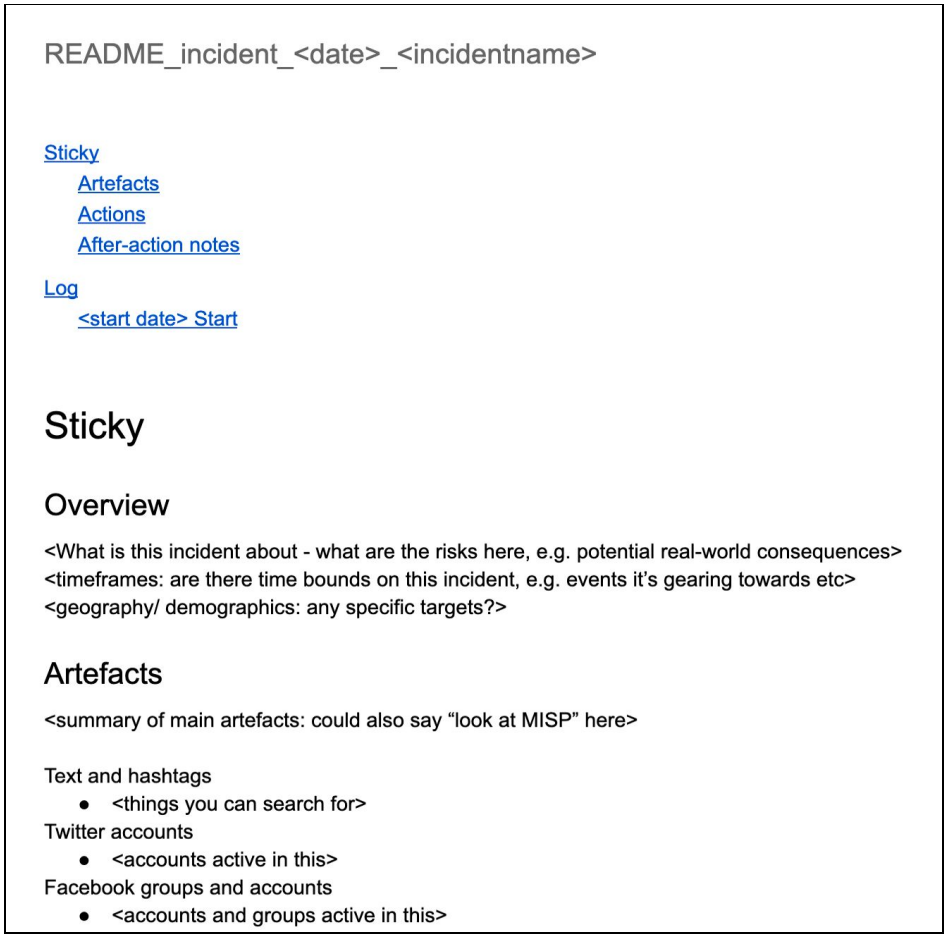
- You need to get information about the incident out to other teams that could do something about it:
    - You've already added an incident to MISP; make sure it's ready to go (question: is there something we need to do to get it out on the feeds?).
    - Write and send notes/reports to the people who can respond
- If you found ways to respond, decide what to do, and check whether you did it
    - If the team found ways it could respond - triage them. Find ways to do the ones you can.
    - Also check on the things you were going to do. Was something done? Chase it up.
- And finally, know when to stop.
    - If you've done as much as you sensibly can, close down the rumor and move onto the next one (there's always a next one).

There are always more incidents, although we're often lucky enough to have a few days without anything major going on. Every morning, one of the leads looks through the list of incidents and decides which ones should continue to be 'live', which we should move to just keeping an eye on, or keep a longer-term watch on in case they flare up again, and which we can close down as unlikely to be active again.

## Small-scale system with a Slack and Googledrive

We've run incident responses armed with nothing more than a Slack group and a Google folder.

With this variant, you still need to track which incidents you're responding to. We used a googlesheet with a row for each incident, giving it a name, a status (live, watching, closed), a start date, an end date (when we closed the response, not when the incident closed), and links to any slack channels and  googlefolders we used to collect and store artefacts, and write up reports in.



README_incident_<date>_<incidentname>

Sticky
- Artefacts
- Actions
- After-action notes

Log
- <start date> Start

## Sticky

### Overview

<What is this incident about - what are the risks here, e.g. potential real-world consequences>
<timeframes: are there time bounds on this incident, e.g. events it's gearing towards etc>
<geography/ demographics: any specific targets?>

### Artefacts

<summary of main artefacts: could also say "look at MISP" here>

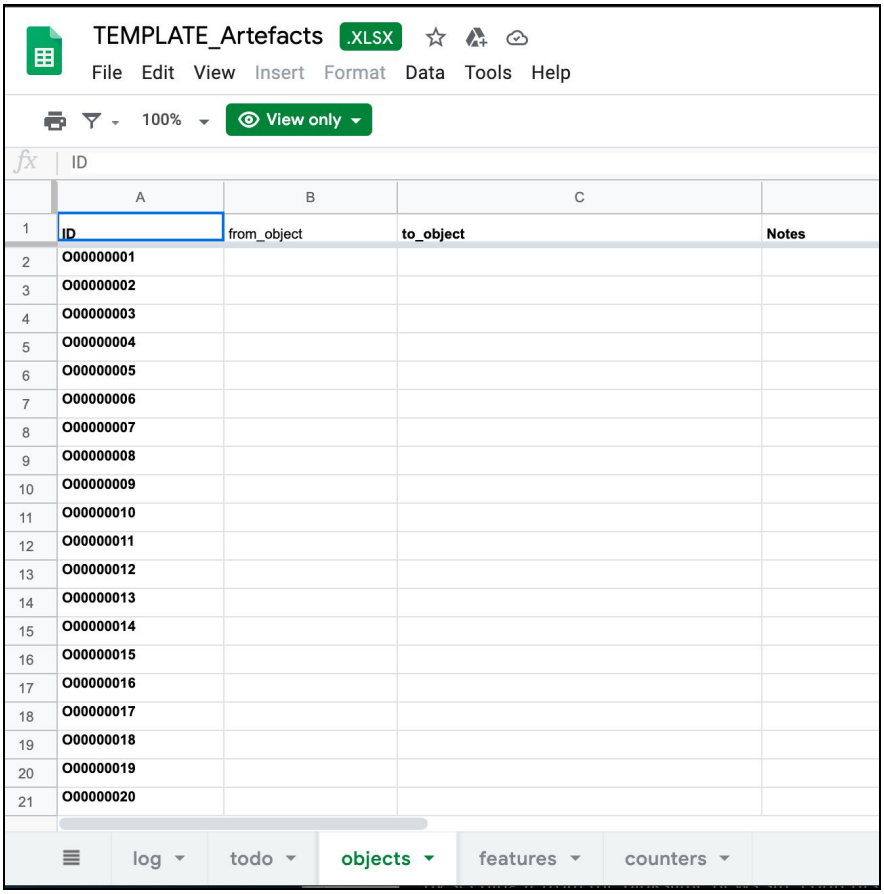
Text and hashtags
- <things you can search for>

Twitter accounts
- <accounts active in this>

Facebook groups and accounts
- <accounts and groups active in this>

Googledoc-based reporting

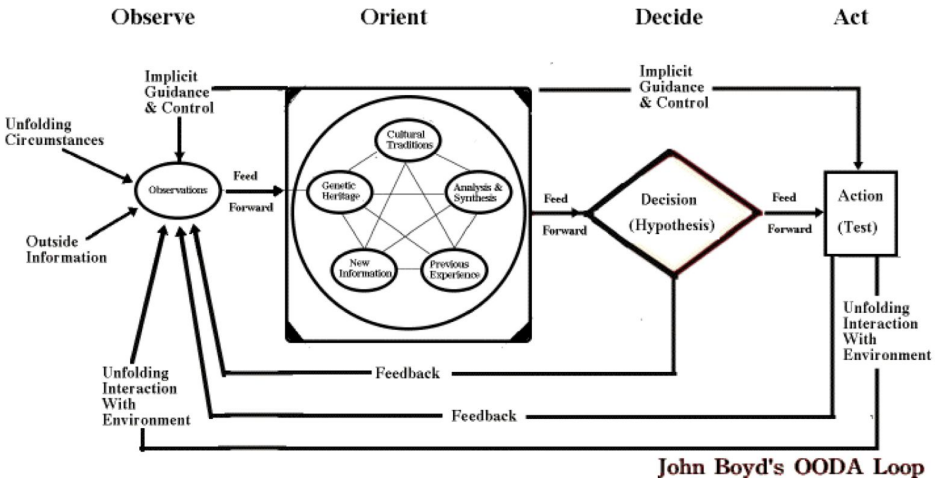
One iteration of these processes used a shared googledrive for each incident, with a folder for images and other artefacts that couldn't be easily copied into a document (videos etc). Within the googledrive was a README file (template above), with sections for artifacts found (because pasting the same image repeatedly is less helpful than giving it a reference number), actions taken, a log of what was found and done on each day of the incident response, and after-action notes when the incident is closed. This is loosely based on some of the shared documents used during crisismapping.




Googlesheet-based reporting

One flaw of the document-per-incident approach was that it became difficult to share and check incident artifacts. We solved this by created a googlesheet template where we could add artifact URLs, then run code to upload them into other systems for automated analysis.

# OODA loops and intelligence cycles




OODA Loop (Boyd)

As we work through incident response, we're going to be mentioning the OODA loop. Boyd's work has been abused for everything from childcare to management theory, but it's still a good way to look at the process from collecting information about the world, through building a "situation picture" that models what you think might be causing those observations, deciding how to act in that situation, then acting and responding to counter-actions in it. First, we'll talk about the "observe" step.