Project Obsidian

Incident Response

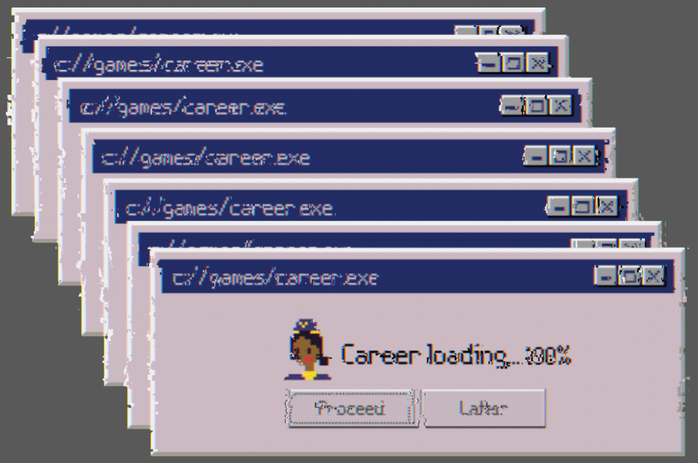
Mise En Place for Investigations

If you don't document it, it didn't happen.
A real-world approach to IR communication.

- aviditas

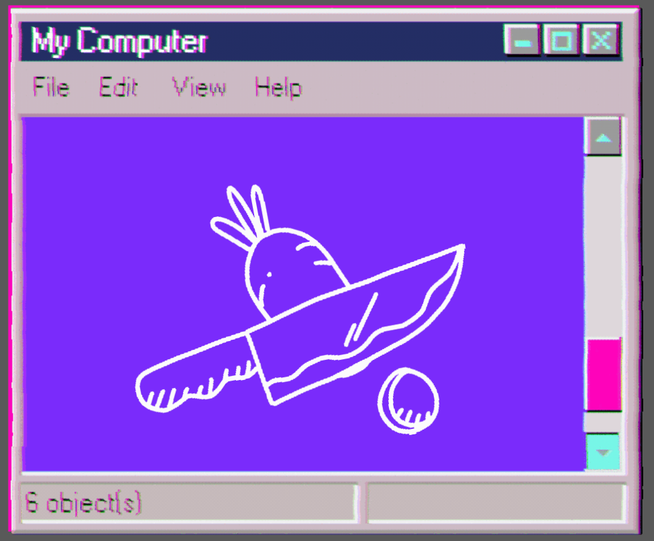
The Incident Response Lifecycle

- Preparation ***- You are Here!***
- Detection / Analysis
- Containment
- Eradication
- Recovery
- Post Incident Activities ***- And Here!***



And a little bit everywhere else too..

What does Mise En Place mean?



It is a French culinary phrase which means "putting in place" or "gather".

It refers to the setup required before cooking, and is often used in professional kitchens to refer to organizing and arranging the ingredients that a cook will require for the menu items that are expected to be prepared during a shift

Mise En Place is separate from the holistic preparation that happens in a restaurant. It is specific to the needs of the chef for that specific day and menu.

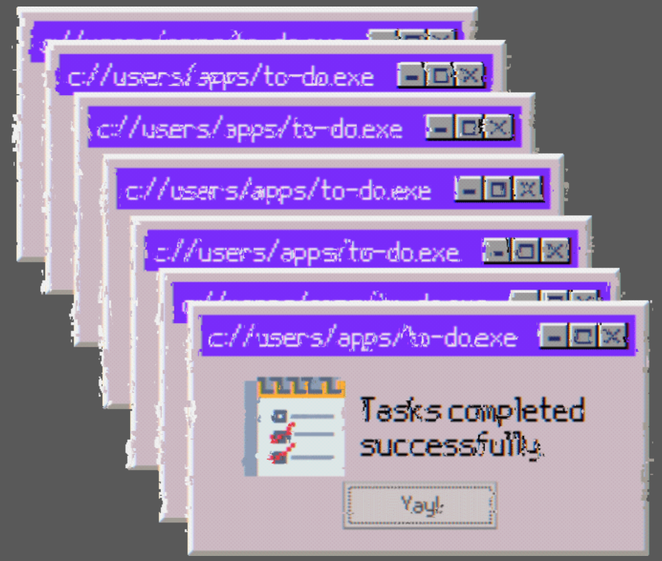
Preparation Hindsight

Before Mise en place, you have to plan and organize, but you don't know what you don't know.

Start with listing out the tools and access you use on a daily basis.

Make yourself a checklist for a normal day and add to it over time.

Slowly organize your list by incident type and then even match to your workflows or playbooks.



Envisioning the End at the Beginning

Requirements First!

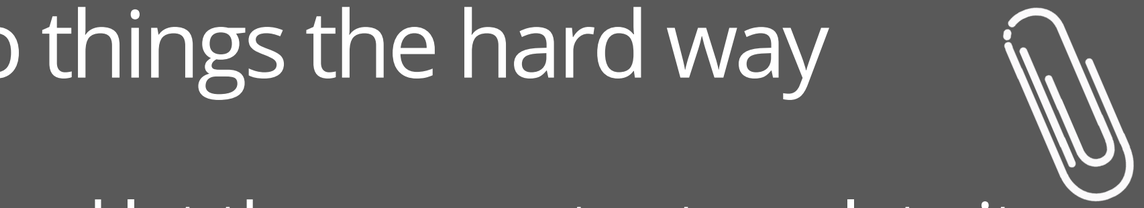
What are your requirements for reporting, lessons learned, and audits?
Are there already templates or playbooks to follow?
Ticket quality guidelines?
If not, then write them for yourself.
List out the required types of information that you will need at the end of the incident.

That is the information you need to be focusing on gathering *as the incident is worked.*

Helpful Tips and Tricks

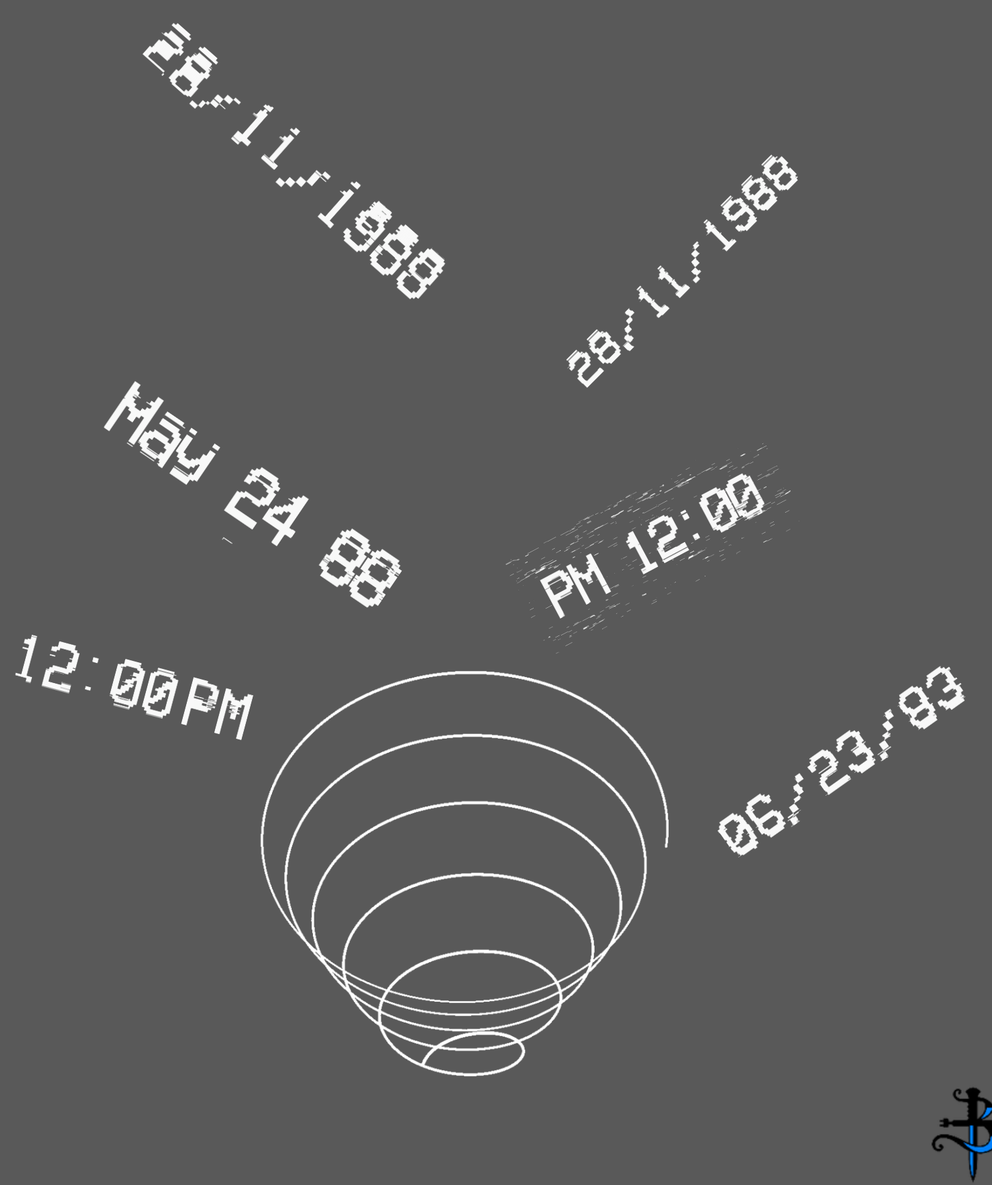
- Clean as you go.
  - Taking 20 seconds to write something down in the case/ticket will save you twice that later.
- If you use non-standard or personal abbreviations, EXPLAIN THEM.
  - No one likes having to spend hours with the auditor.
  - And the auditor prefers to be able to just read your notes.
- Write notes for yourself like you will get amnesia tomorrow.
  - Because you can and will forget things you don't deal with every day.
- Don't try to memorize what you can document.
  - Unless that's your superpower.

It looks like you are trying to do things the hard way

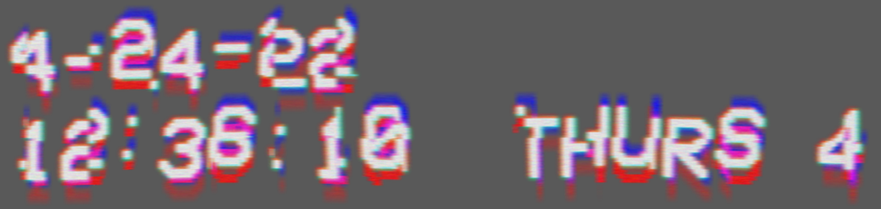


- Short keys! Type an abbreviation and let the computer translate it for you.
  - AutoHotKeys is my personal favorite but can't always get it.
  - Code them! If that's your jam at least.
  - VIM? I wouldn't know but people keep telling me about it.
- Clipboard management.
  - You copy so much during IR, get a tool that helps you out.
  - Be sure to set it up securely and get approval.
  - I recommend having it auto-clear at the end of each shift at minimum.
- You really should have an org-wide password manager.
  - KeePassXC is usually an easy approval otherwise.

Building a Timeline Framework



Consistency is Key!



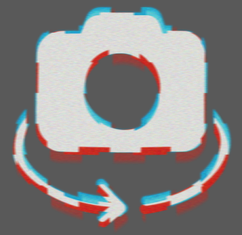
Put the time in Timeline. Just stay with UTC if you can.
UTC can't hurt you the way that local time zones can.

Pick a format for timestamps, IPs, geolocations, users, hostnames, event data... etc. then stick with it.

Side note: This also applies to a term or word for a thing, pick one and use that throughout your incident.

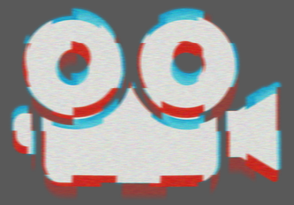
Swapping any of these out at the end is just not worth the time when you can prevent it from being an issue at the start.

Know Your Audience



Your timeline has two main ones:

- An equal or peer | technical
  - They care about your log data and detailed information
  - Think csv files and case attachments
- A manager, stakeholder, or executive | layman
  - They want to understand what happened when... but generally so
  - Think timestamps + a single line of data



Let the Computers do the Work

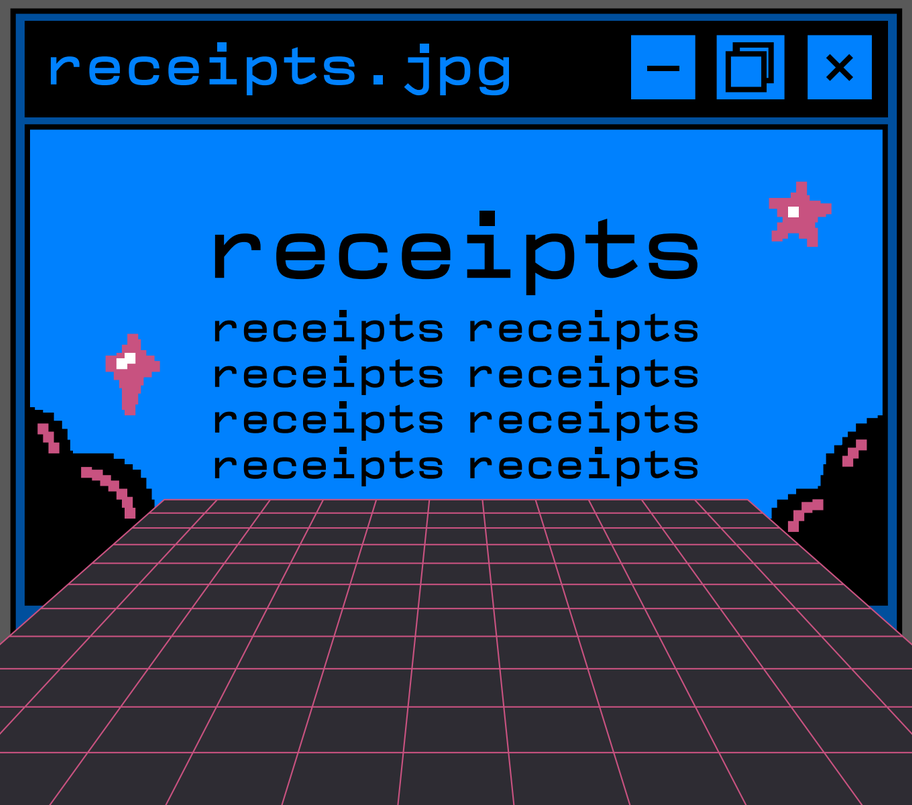
If you can think of a niche, there's an IR timeline tool for it.
I won't get into naming DFIR tools, the forensics team has that more than covered.

For incident *handling* this seems to be the shortlist:

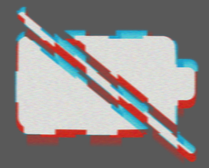
- Ain't nothing wrong with plain text or markdown
- Excel has its place like the inescapable passage of time
- Jupyter Notebooks + Mito if you are feeling fancy
- LOTL: Find and use the built-in tools for your logging or security software
    - MS Defender Timeline, Splunk local, Kibana, Arkime...

Demo Time

What do good notes look like?



Good Notes = Better Sleep for Everyone

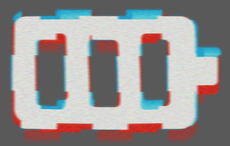


If you are being grilled by a cranky senior analyst, can you answer their questions?
More importantly, *why are those questions being asked?*

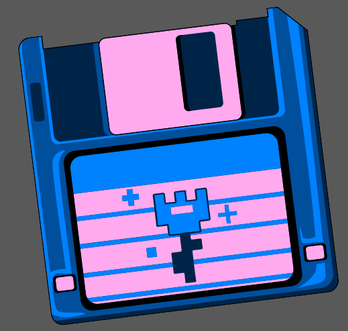
During the IR investigation you need to:

- Pinpoint the root cause
- Find and include the data points needed for re-scope, tuning, and lessons learned

If the notes can't explain the why you did a thing, you need to include your reasoning and proof.



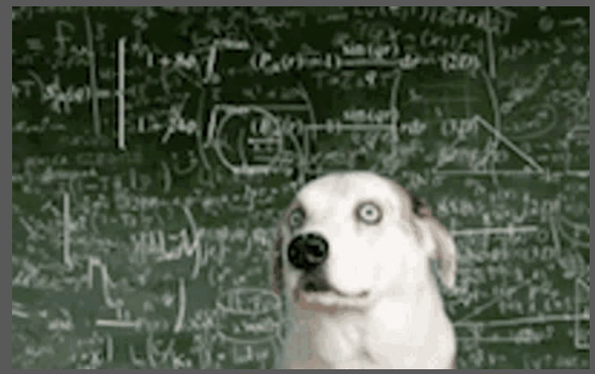
Notes are for Your Protection



If something is missed or you make a mistake, someone else should be able to follow your thought process.

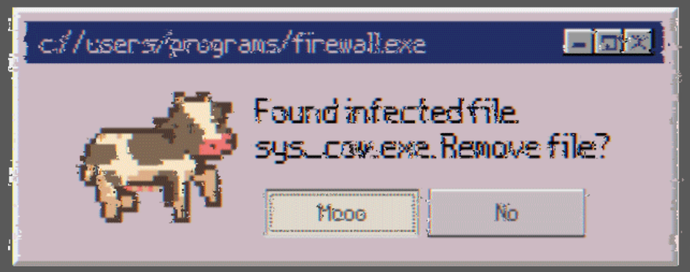
Audits can be miserable if you have to try and pull from memory or locally saved rough notes.

Think of notes as your save button. You don't ever want to have to go back and redo hours & hours of work.



If you aren't sure about an IOC or event logs, note that as you record it. 6 hours into IR, your memory of the 5th IP address out of the 105 you saw will be sketchy at best.

Demo Time


c://users/programs/firewall.exe
Found infected file.
sys_cow.exe. Remove file?
Mooo
No


Color Commentary
&
Play by Play

Are you sick of the analogies yet?

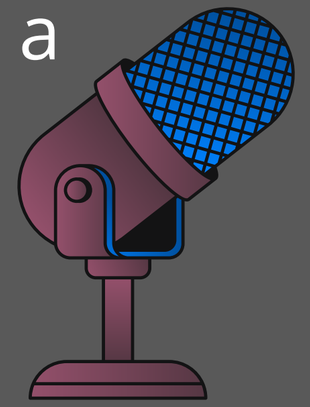
In the land of sports ball, there are typically two announcers.

- One does the play by play, describing the events as they unfold
  - Someone with only that information should be able to follow the course of the game.
- The other does color commentary, providing additional information around the players and actions.
  - This is typically opinions interlaced with other factual sources.
- Having both together works best.
  - This sets the facts along with expert opinions so that both the average listener and the avid fan can get what they need.

Now Apply that to Notes!

Color Commentary is usually just for the internal security team visible notes on incidents. So be mindful of professionalism but include your honest professional opinions.

Then there are the outward facing communique types that need a neutral tone to prevent unwanted drama. Play by Play time!



Status updates - aka we are working on the thing so please stop bugging the people doing the work
End of shift/day/put a pin in it - a summary of what has happened and is known at that time
Client updates - status updates but even embrace the vague

Be very sure you know who can see what.

We are all Vulcans here

As a rule, on outward facing notes there are no opinions, only facts.
Yes, you know that this is a breach/compromise but if you say that in an email without the 'proper' wording, your legal team will be very not happy with you.
Unless it is literally your job to make that decision, don't.

Possible, potential, popped... these are your favorite prefixes.

Soft wording describes the fact without using words that have a regulatory and legal meaning; so, security event not incident, unauthorized access not breached or compromised.

It can seem silly, but if you play nice with legal, they will be a great ally.

Demo Time

The Ending Approaches

TL;DR

The Preparation and Lessons Learned stages of IR are NOT just for management and the other departments.

Do your own individual versions of each and your work quality + general stress levels will thank you.

Mise En Place self-checklists can help identify tool, knowledge, access, and communication gaps you have.

UTC is best time.

Write what you do & think as you do & think it. Smash that save button.

Be nice to Legal and they will be nice back. I promise.

References

Mise en place - Wikipedia
https://en.wikipedia.org/wiki/Mise_en_place

Thank you!

Join the conversation
https://discord.blueteamvillage.org