Project Obsidian

Incident Response

Eating the Elephant 1 byte at a Time

How to know what you don't know, quickly.
IR handling: Scoping, Triage, and Communication

- aviditas

The Incident Response Lifecycle

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

The Incident Adrenaline Rush!

And the fire alarms are blaring..
And the executives are glaring...
And the analysts are swearing....
And everything is just completely.....

overwhelming.

In the midst of panic

Under the haze of harrowing horrors, you will find yourself asking yourself existential questions...

- Why is this happening (to me)?
- What is even going on here?
- Where is anything?
- Who am I?
- When will I get to go home?

Congratulations!
You are asking the right questions, just to the wrong audience.

Why is this coming to me?

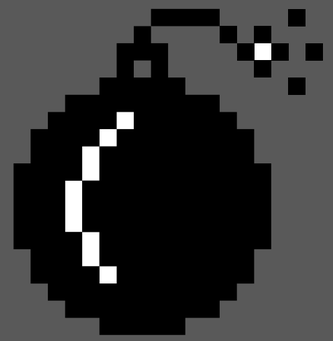
Open up the Security Incident Plan and make sure that you have all of the info from the reporting party. Squeeze the stone dry!

Who ya gonna call?

Seriously, who? It's 3 am and the Incident Response policy hasn't been updated since it was made. Comms plan?! Maybe?

Who am I?

Make sure you have what you need to do your job. Access is like backups, you have to test them regularly to be sure.



What is happening?

Let's go and find out!

When do I get to leave?

That's a 'you and the people who pay you' question.

But first take a deep breath

Incident response can be high stress and intense at the best of times.

Make sure that you hydrate, take breaks, and eat snacks.

Adrenaline wants to keep you in a hyper focused state.

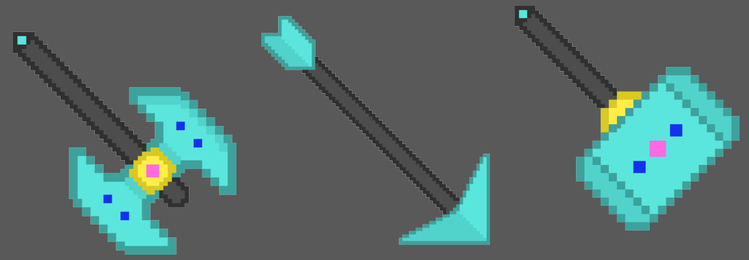
The more you prepare both technically and mentally, the better you will do and feel.

It's Dangerous to Go Alone...

You have support!

Your coworkers should be your first support line. (for work)
The internet has many answers for those who seek them.
Read error messages and existing documentation.
Find or build a non-work support network.

Remember it's okay to be asking a ton of questions but make sure you are doing due diligence first. Include where you looked first with your question(s) and share your knowledge back out to others.



Break down the details you have & apply questions

What/Who?

- Searchable Specifics: hostnames, usernames, file/software names, email addresses, IPs, Subject lines, URLs, alert queries...

Why?

- Motivation matters. If there's not even a basic answer, start looking at scale & checking for 'normal'.

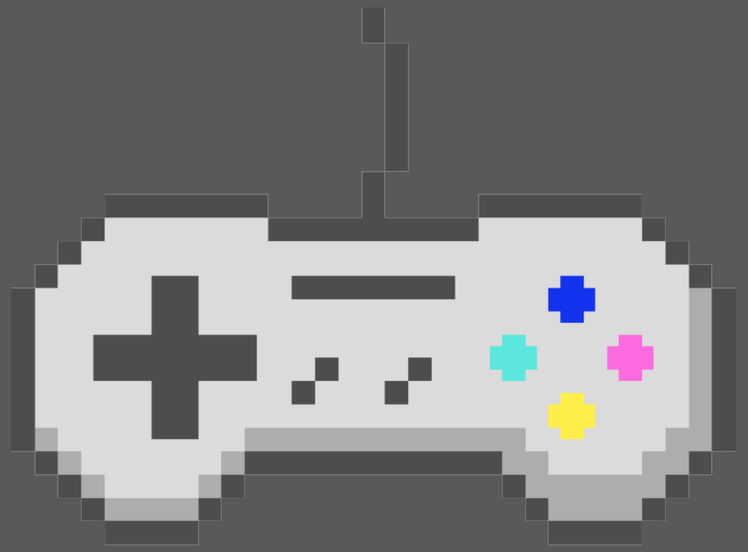
Where?

- Identify the probable sources or data locations

When?

- Exact is great, but windows are acceptable.

To the SIEM!



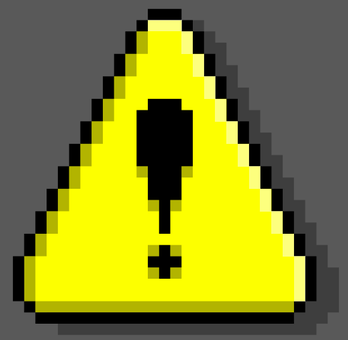
Filters are your friend

Yes

Ignore

Cancel

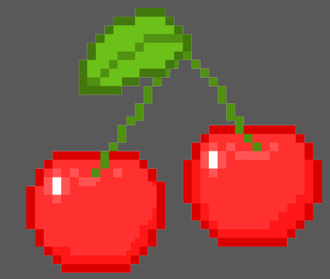
Start



Run

No

It's A R T !



There are two fundamental search methods for IR analytics.
Both have their place and different tools can be easier to use with one or the either.

Painting the picture:
You have a faint mental vision (hypothesis) of the end result, and you use the data to paint it. Going to specific sources for what you need.

Whittling away the wood:
You have the data and a means to remove what you don't want to see. With little to go on, you can reveal the underlying 'interesting' result.

SIEM Speed Run

Time for Quest(ions)

Thank you!

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