Asking Questions and Writing Effectively

Christopher Lopez
@L0psec

Who?

Father

SOC Analyst
Blue Team Investigator

Always Asking
Questions

Agenda

Investigative Questions

Writeups

Tools to be an Awesome Investigator

- Your mind:
  - Including your **questions**, biases, perspective, and experiences.
- Somewhere to take notes:
  - Paper and Pencil
  - Any Text Editor
- A loosely defined process
- Team members

The Investigation Engine

Questions

Artifact collection

Rabbit holes

Compile Findings

Form conclusion

Documentation

The Scientific Method

Observation

Question

Hypothesis

Experiment

Analysis

Conclusion

Questions

What?

Why?

When?

Where?

Who?

How?

What?

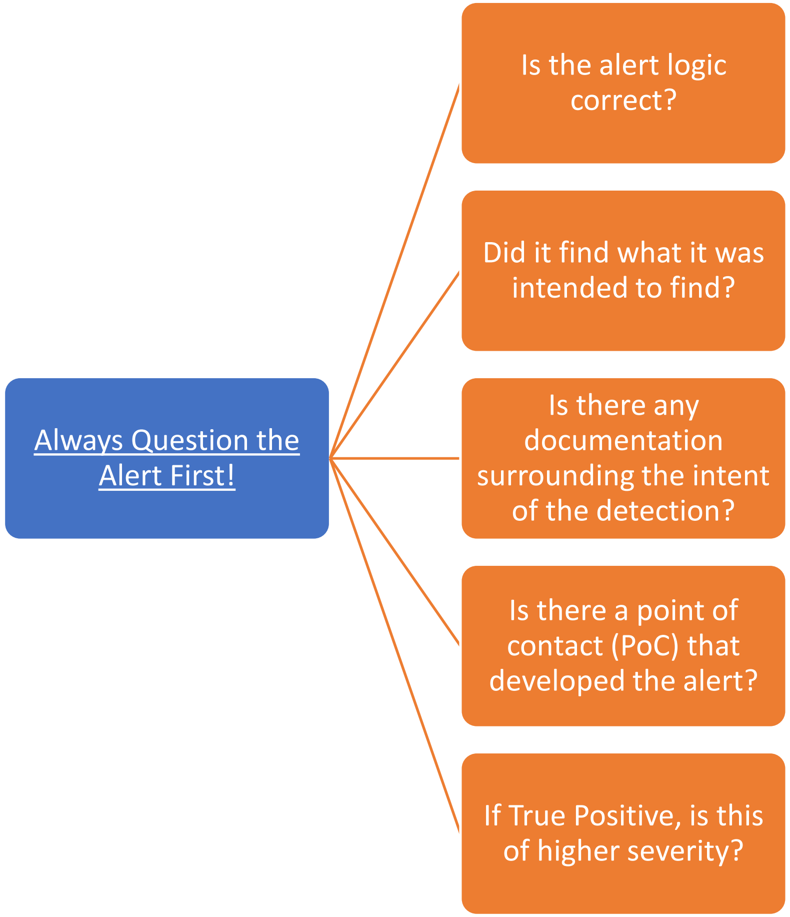
SIEM detection?

Threat hunt idea?

Recent breach report?

New organizational process?

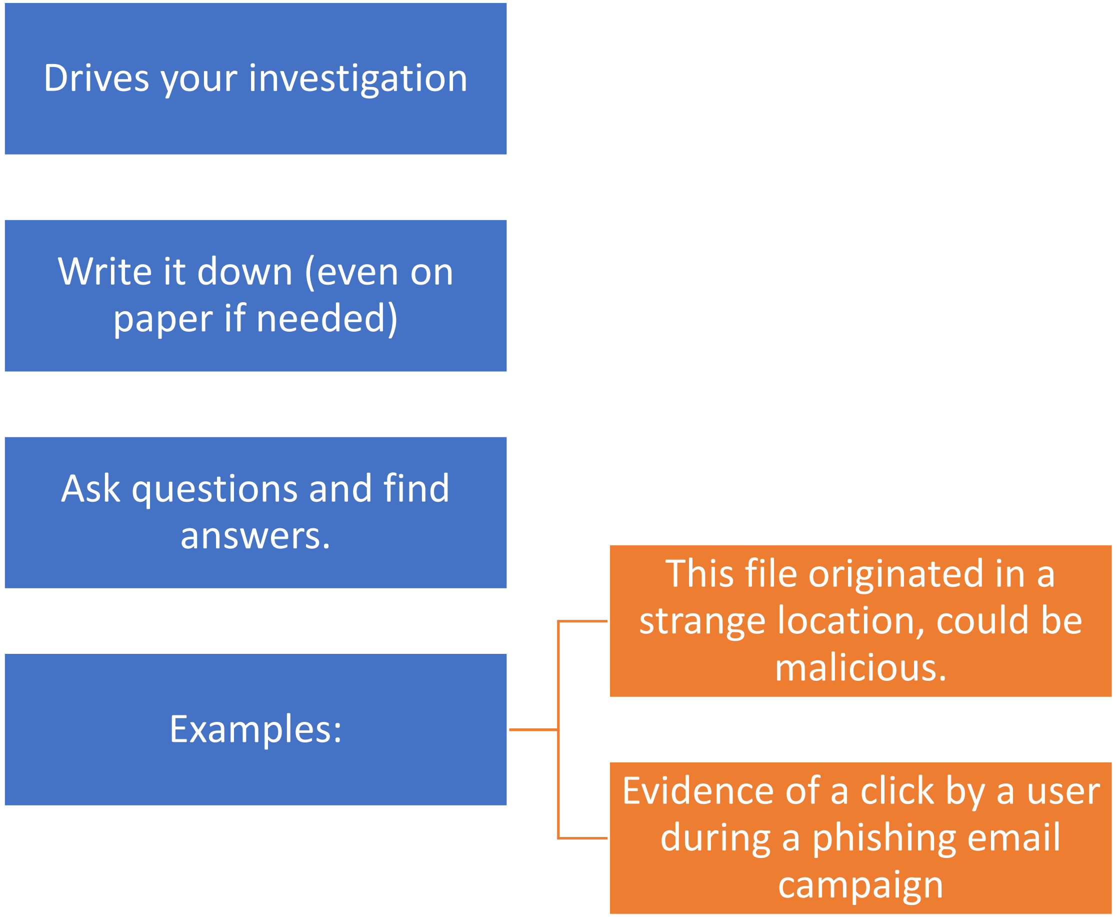
What? - Always Remember



Always Question the Alert First!

- Is the alert logic correct?
- Did it find what it was intended to find?
- Is there any documentation surrounding the intent of the detection?
- Is there a point of contact (PoC) that developed the alert?
- If True Positive, is this of higher severity?

Why? - Your Hypothesis



Drives your investigation

Write it down (even on paper if needed)

Ask questions and find answers.

Examples:

- This file originated in a strange location, could be malicious.
- Evidence of a click by a user during a phishing email campaign

Building your Hypothesis

Falsifiable

Testable

Scope?

Lesley Carhart @hacks4pancakes, WWHF 2020, (Most) Everything You've Been Told About ThreatHunting is a Lie, and That's Okay"

Example Alert and Hypothesis

Alert:

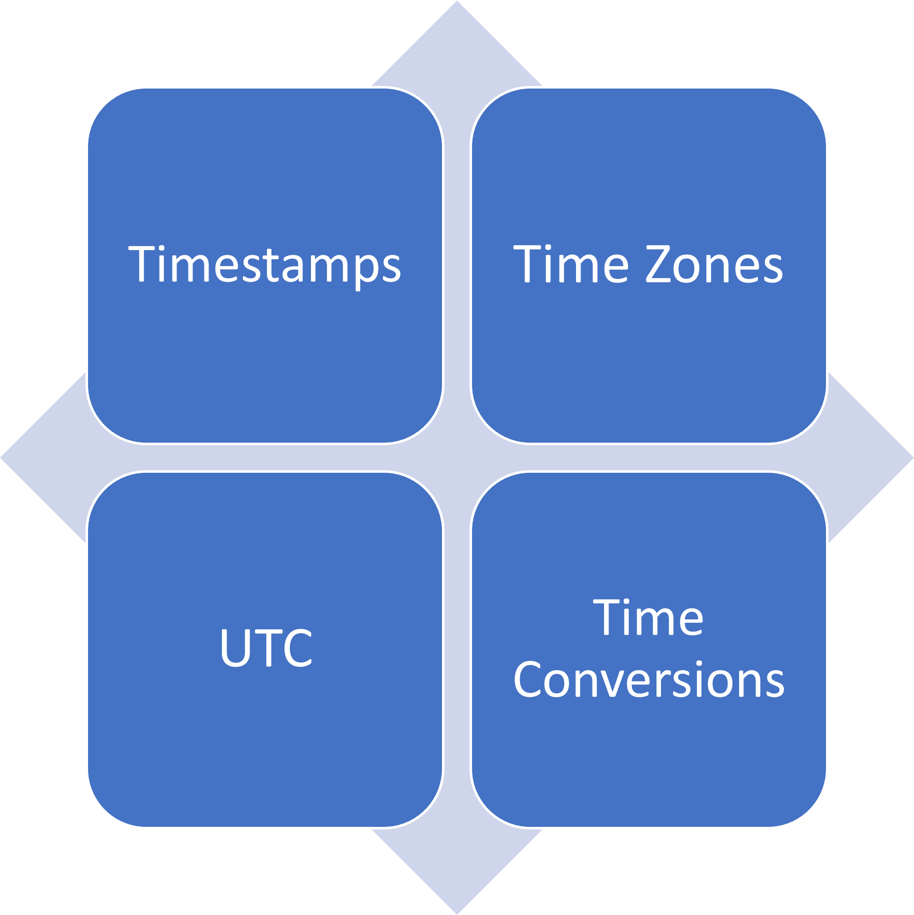
June 5,2020

AV detected a potentially malicious file in a user directory.

Hypothesis:

File did not execute.

When?



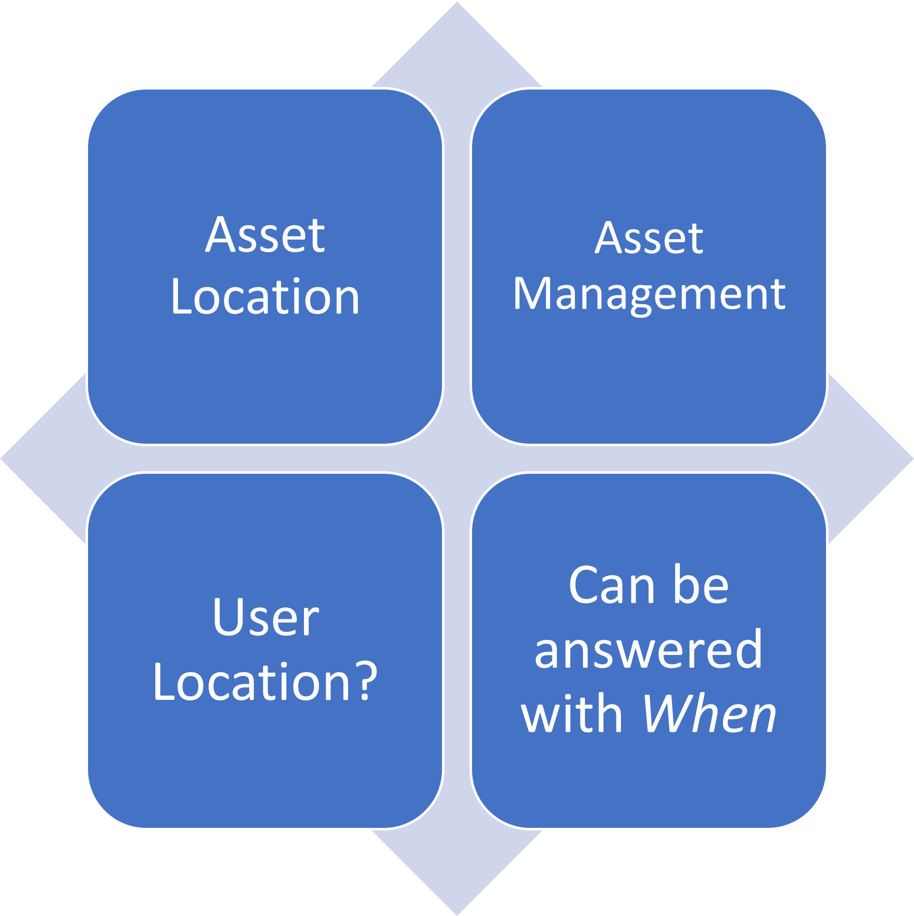
Timestamps

Time Zones

UTC

Time Conversions

Where?



Asset Location

Asset Management

User Location?

Can be answered with *When*

Who?

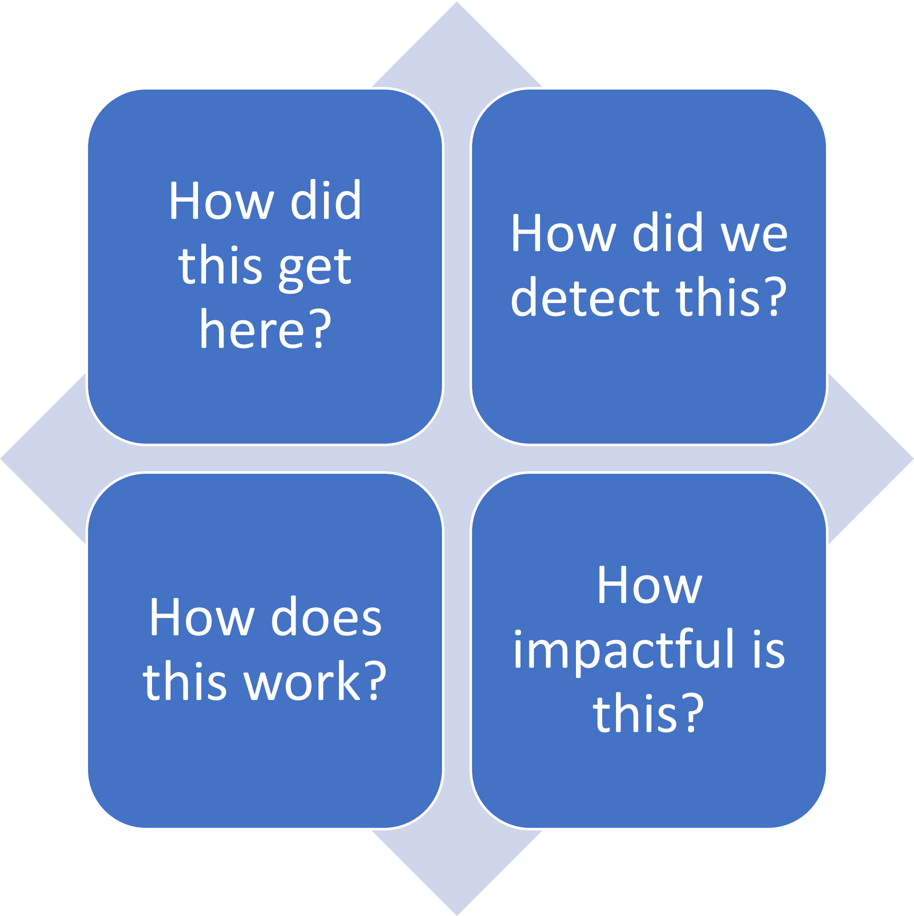
Attribution

Threat Intelligence

Insider or Outsider

Employee, Vendor, Co-Worker?

How?



How did this get here?

How did we detect this?

How does this work?

How impactful is this?

Investigation Writeup

- An analyst’s effort is reflected through their documentation.
  - What actions did you take?
  - When did you take these actions?
  - What answers did you obtain?
  - Is escalation required?
  - What is your conclusion?
    - False Positive? True Positive? False Negative?
- Always include a BLUF
- Provide Contextual data
  - Timestamps, User/Endpoint Information, OSINT data to support claims.

BLUF

- Understand your audience
- Bottom Line Up Front
- Three C’s
  - Concise
  - Clear
  - Correct

Writeup Importance

- Your writeups can invoke change in a process.
  - Did you write it with that expectation?
- Can someone replicate the actions you took?
- Did this investigation lead to a potential improvement in detection?
- Would senior leadership be able to use this writeup to address any concerns?
- Did you document your findings and/or conclusions in a Wiki?

Resources

- Chris Sanders’ Investigation Theory Course
- Robert M. Lee and David Bianco, “*Generating Hypotheses for Successful Threat Hunting*” https://www.sans.org/reading-room/whitepapers/analyst/generating-hypotheses-successful-threat-hunting-37172
- Daniel Kahneman, “*Thinking, Fast and Slow*”
- James S. Major, “*Communicating with intelligence : writing and briefing in national security*”

Thank You!