Project Obsidian

Incident Response

It all starts here, scoping an incident

Background

Investigator Mindset

1. Create a hypothesis
2. Understand what evidence you need to prove it
3. Determine if the evidence is attainable
4. Review and analyze the evidence
5. Confirm if your hypothesis is:
   - Correct
   - Incorrect
   - Unable to be determined

Lifecycles

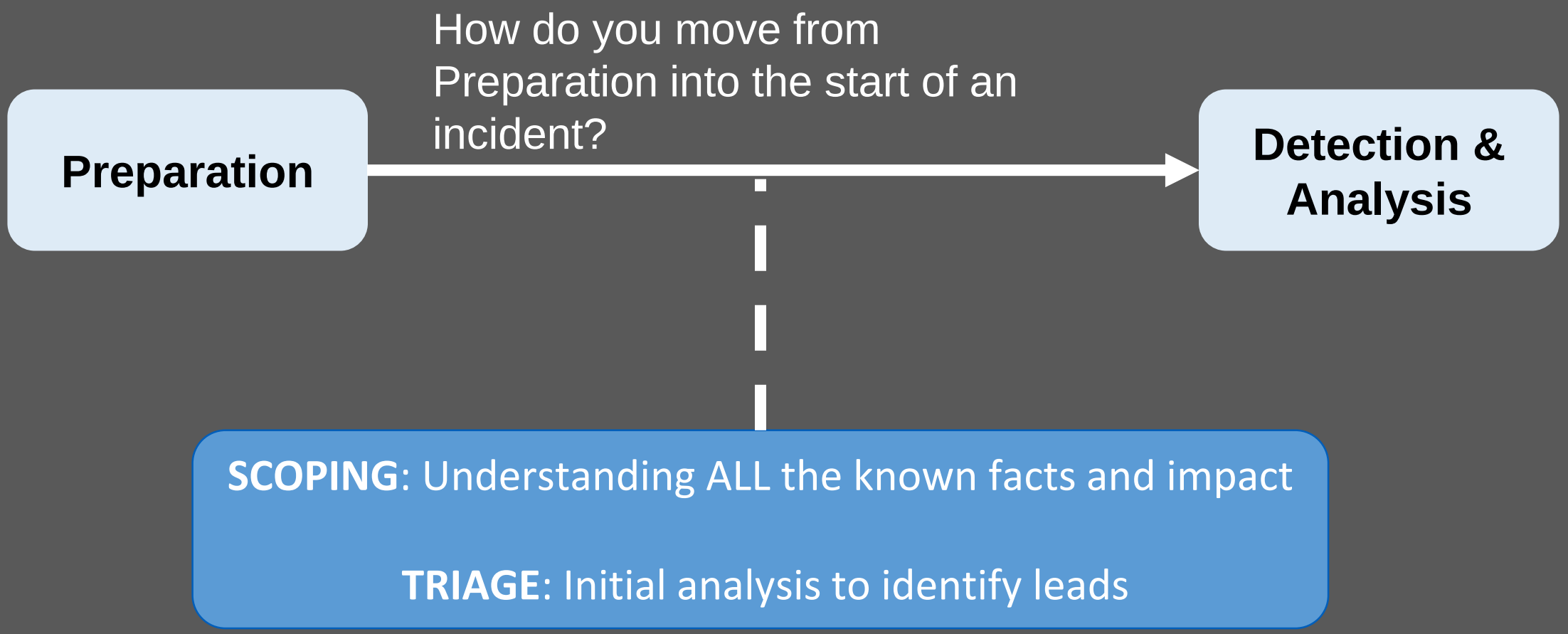
Incident Response

- Preparation
- Detection / Analysis
- Containment
- Eradication
- Recovery
- Post Incident Activities

MITRE

- Collection of adversary tactics, techniques and procedures (TTPs)
  - Tactics
  - Techniques
  - Procedures

How do I start?



Scoping

Incident Scoping

- Goal
  - Determine if the event should be considered an incident.
    - Have you seen this before?
  - Understanding the incident and what needs to be done
- One analyst should be dedicated to taking notes from the meeting/ticket/etc.
- Use templates for scoping notes, have prepared questions to ask (You will forget)

Incident Scoping (cont'd)

- Setup a briefing with team members:
  - Additional notes about the incident and organization
  - Evidence sources
  - Confirmed objectives
  - Next steps for each IR team member

- Establish a communications cadence
  - Daily? Every few hours?

Kill Chain 1 Scoping Notes Template

Triage

Evidence Collection

- Collection of evidence through:
  - Imaging Software
  - Triage Scripts
  - Security Consoles
  - Log Files
  - Virtual System Files
- Provision or obtain access to data sources such as consoles
- Clear instructions on how to preserve and prepare
- Preplan for analysis, expand the timeframe of investigation

Triage Analysis

- Organize and document evidence collected and associated data
- Don’t rush into an investigation without a plan
- Establish a clear task list
- Objectives should give clear boundaries on what to investigate
- Utilize indicators to identify TTPs associated with them
- Write It Down:
  - Summarize what you are seeing? Not just the bad
  - Did anything standout?

Finding Evil

- Malicious behavior may not always be identified before IR is engaged.
- A baseline of expected activity will make it easier to identify suspicious behaviors
- Common indicators:
  - Rogue Connections
  - Unusual Processes
  - Unusual Services
  - Rogue Accounts
  - Unusual Files
  - AutoStart Locations
- Use the hypothesis approach to set end points. There will likely be several paths to follow. Note them down, but finish your current hypothesis

Findings

- Findings should be identified with at least the following:
  - Timestamp
  - Event Description
  - Data Source
  - Including query or procedure
  - Context (Who, what, where, when, why)
  - Code (Filepath, registry entry, command)

Writing your findings

- Write out findings in “report format”, this eases the process of writing a report and allows you speak on findings during a conversation:
- Understand the timestamp of your data source and always try to convert to UTC when possible
- Develop a consistent timeline with normalized timestamps
  - Trust me it makes you life so much easier!

Kill Chain 1 Investigation Notes Template

Final Advice

- Take a breath and pat yourself on the back! Investigations are tough and can take a lot out of you
- Step away every now and then to regroup
- Know your limits
- Ask for help

Thank you

Join the conversation

https://discord.blueteamvillage.org