PLEASE DOWNLOAD IF YOU DID NOT RECEIVE THE LINK BEFOREHAND

http://bit.ly/2EKvnfk

DEFINING TTPS

BY MONTY ST JOHN

Monty St John

Who is this guy?

- 25 years of security and analytics – physical, investigations, information, computer forensics, reverse engineering, threat intelligence
- Two decades supporting federal, state, and local LE while in uniform

Forensics and Threat Intelligence

- Better part of past decade acting as a key member of forensic and TI teams deconstructing, analyzing and providing insights into threats and how to thwart them

TACTICS - TECHNIQUES - PROCEDURES

PATTERN MATCHING MAGIC

Let's talk definitions for a moment

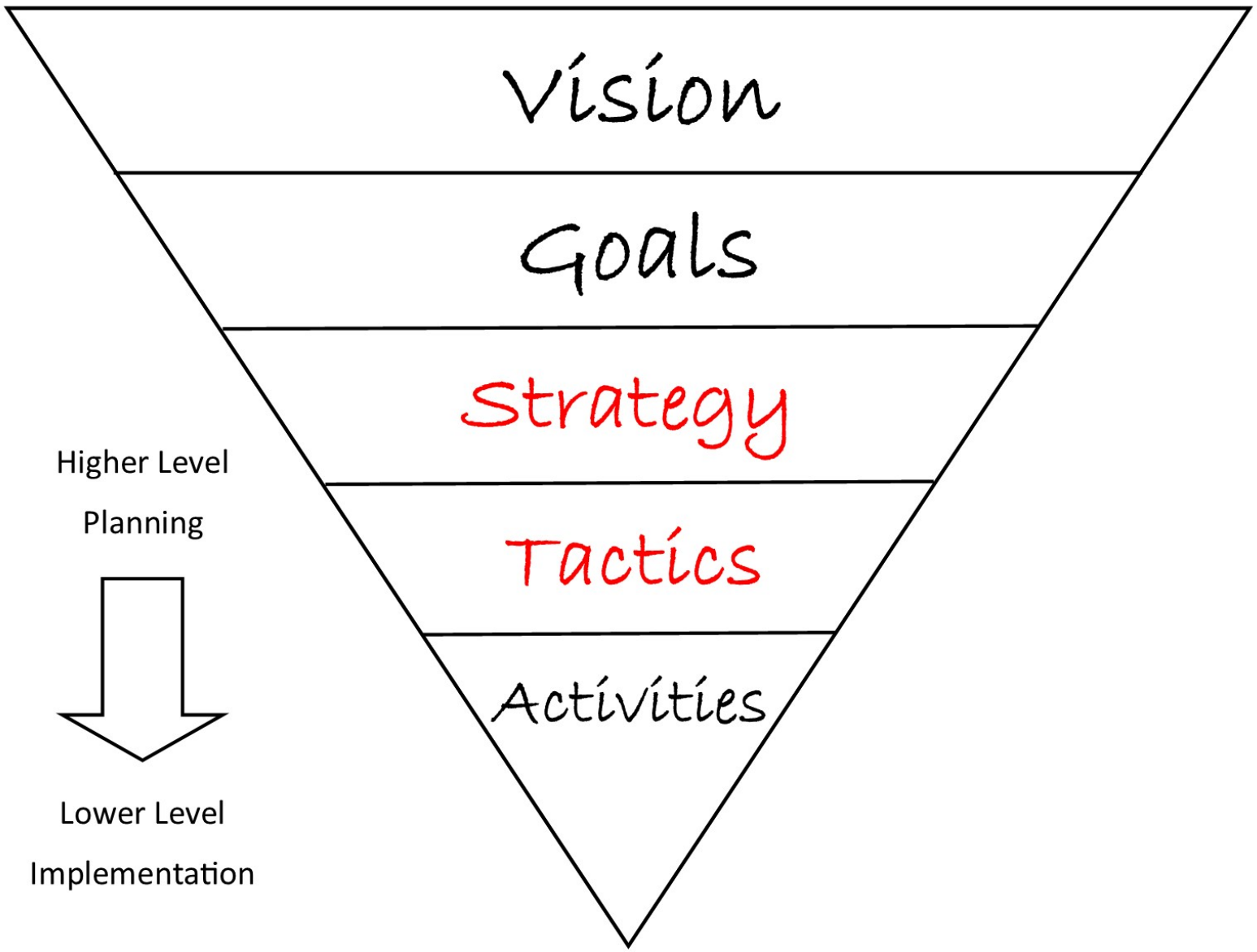
Tactic

Action or method that is planned to achieve a specific objective or goal

Just to contrast:

Strategy

A plan or series of maneuvers to achieve an objective


Vision
Goals
Strategy
Tactics
Activities
Higher Level
Planning
Lower Level
Implementation

Let's answer some questions (discussion):

- Why is it important to identify the tactic employed?
- What can I learn from the tactic about the adversary?
- What can I understand about myself?

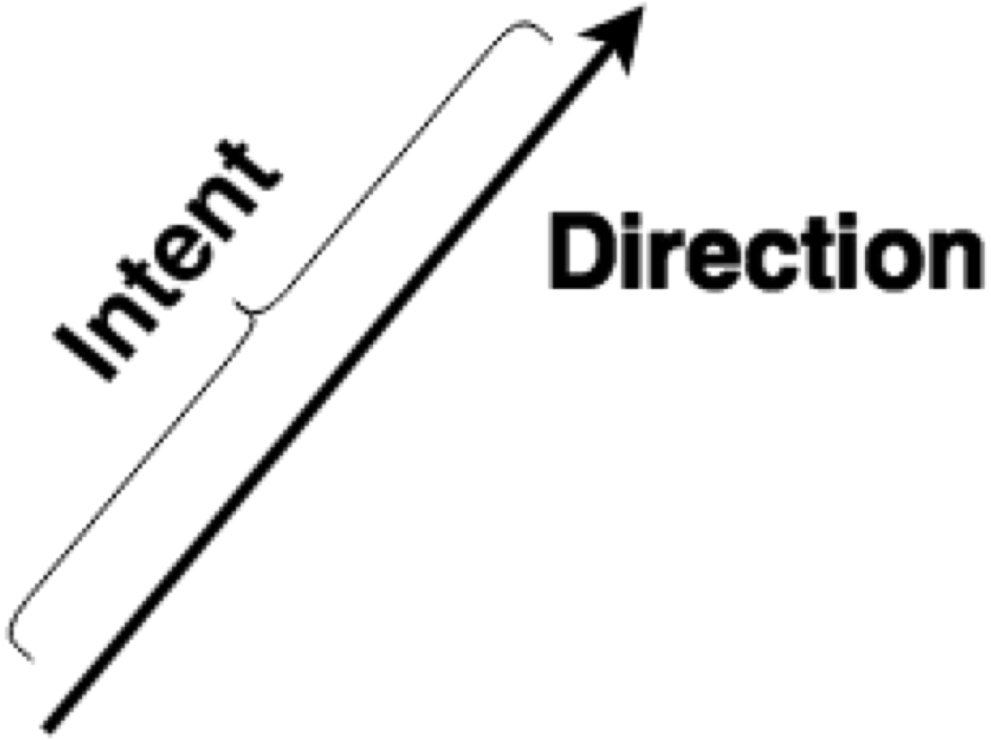
Four important takeaways from tactics:

- Vector
- Mechanism
- Medium
- Operation

Vector

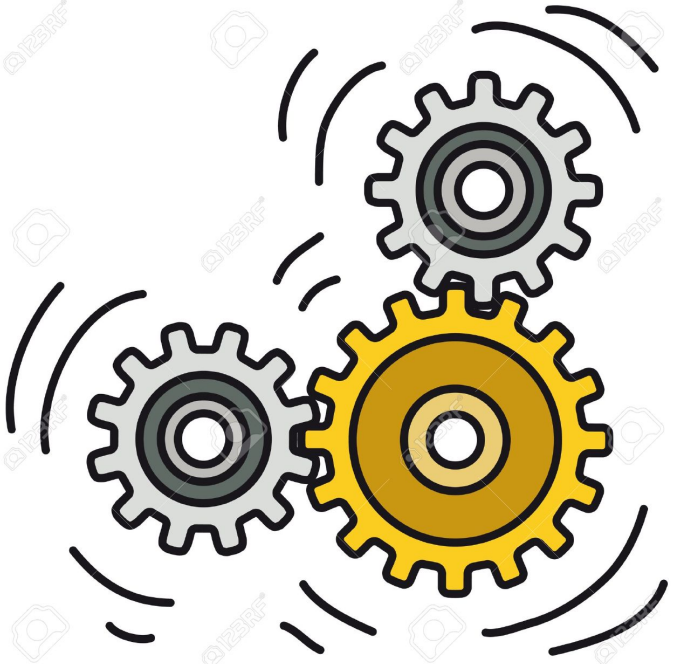
Direction and magnitude.

For us (intelligence), direction and intent.



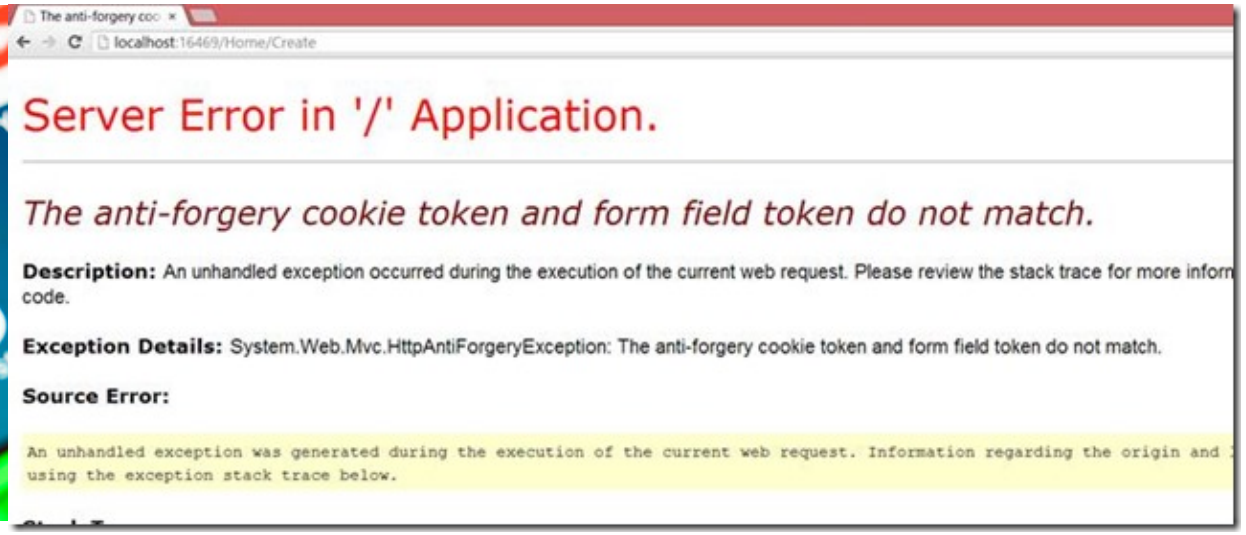
Mechanism

The interactions and influencers, such as Bluetooth, USB, Email, and so on but also password recovery, update methods, account lockout and other mechanisms.



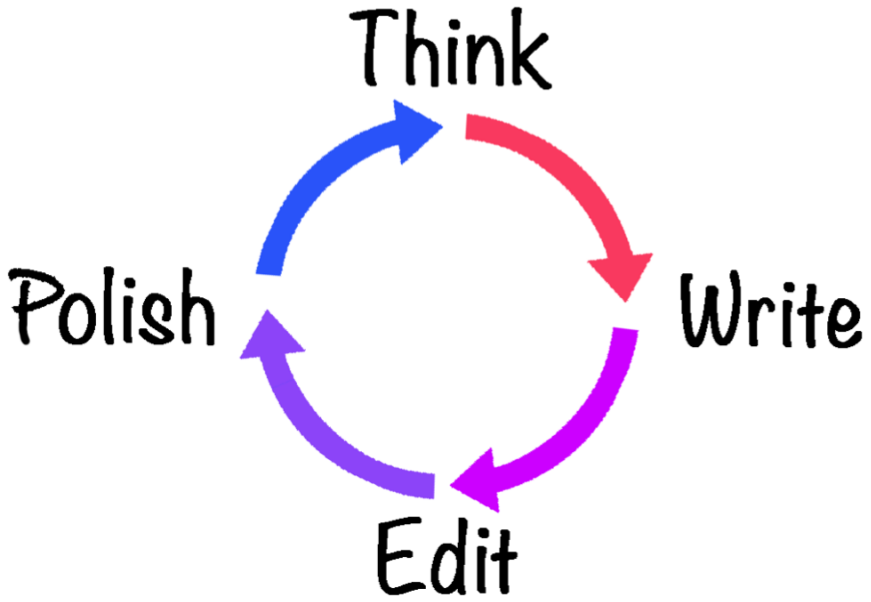
Medium

The path or the surface the tactic employs.

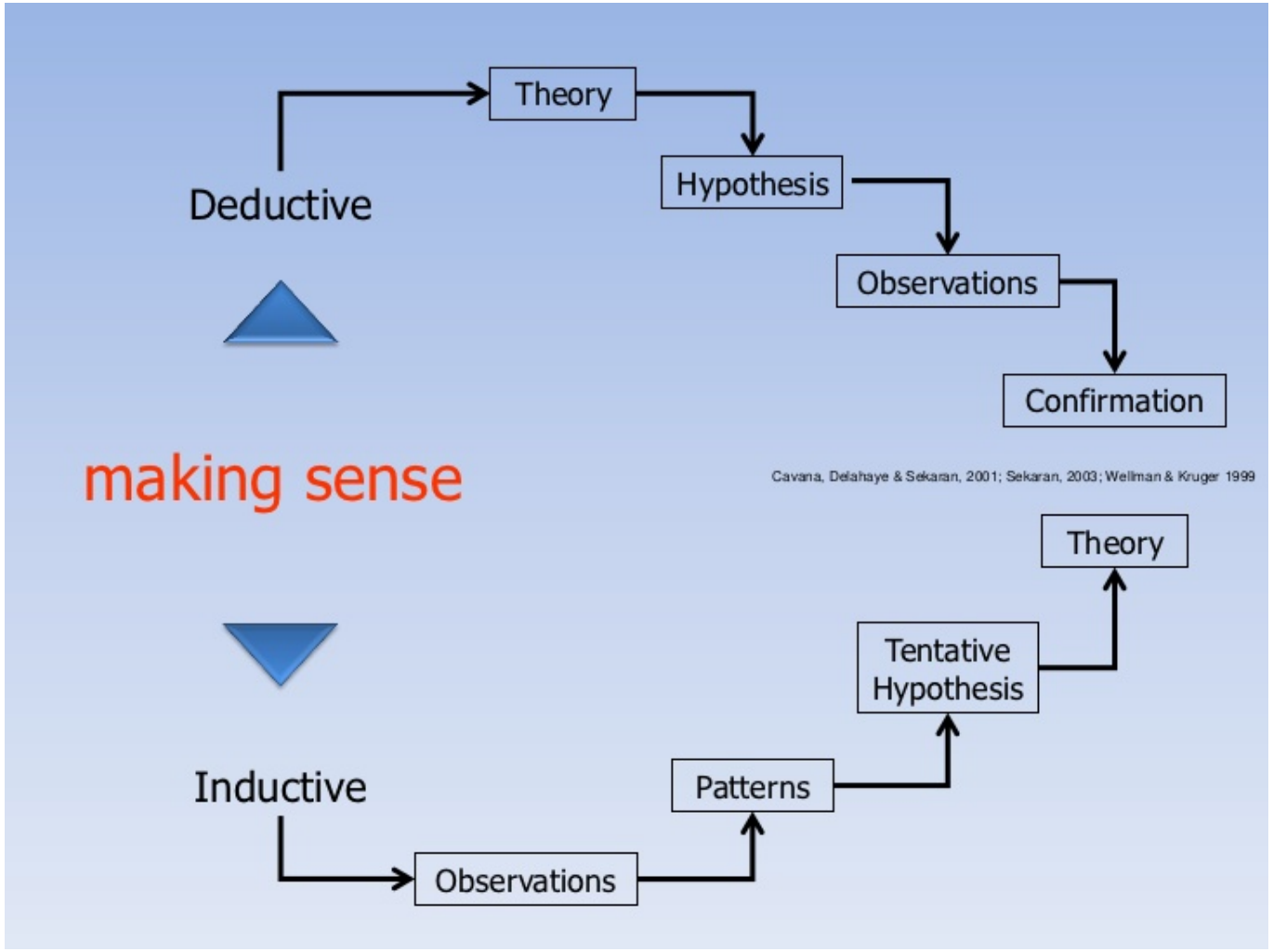


Operations (or Tasks)

The actions taken for the tactic to be employed. Operations and techniques are tightly intertwined.



Workshop I - Operations



Deductive vs Inductive Profiling


From:
Amazon <management@mazoncanada.ca>
on behalf of
not an Amazon email address
(note the missing A in Amazon)
To:
@sheridanc.on.ca
Cc:
Subject: Suspension
amazon.com
Dear Client,
Generic non-personalized greeting
We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.
To confirm your identity with us click the link bellow:
https://www.amazon.com/exec/obidos/sign-in.html
Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"
Sincerely,
The Amazon Associates Team
© 1996-2013, Amazon.com, Inc. or its affiliates

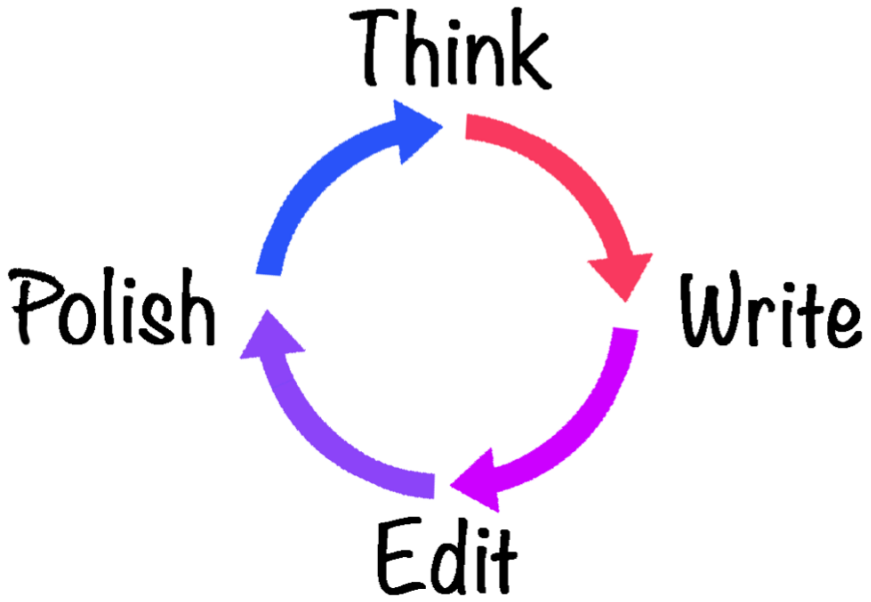
What tactic is in play?

What is the vector for this tactic?

What mechanism can you identify?

What medium is in use?

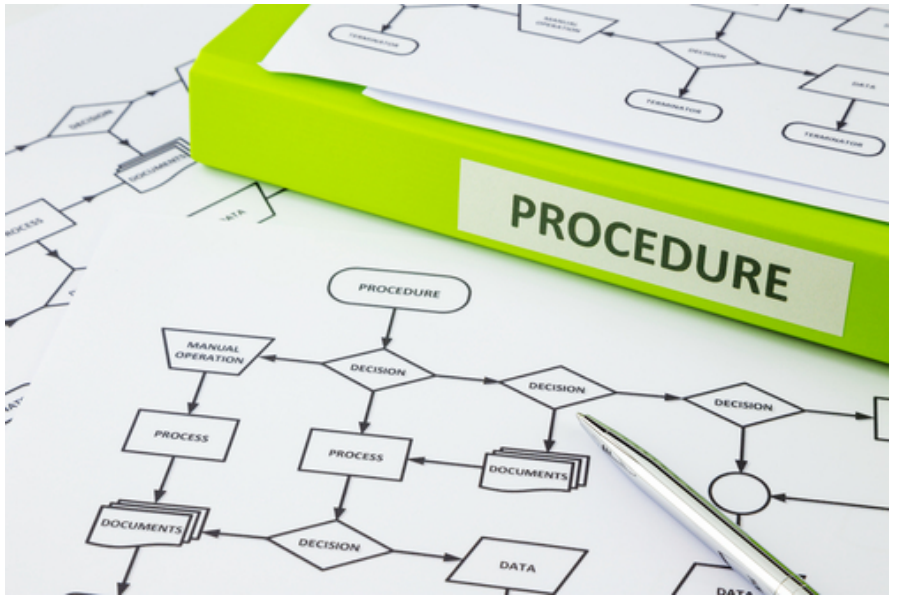
What operations were employed?



Workshop II - Tactics

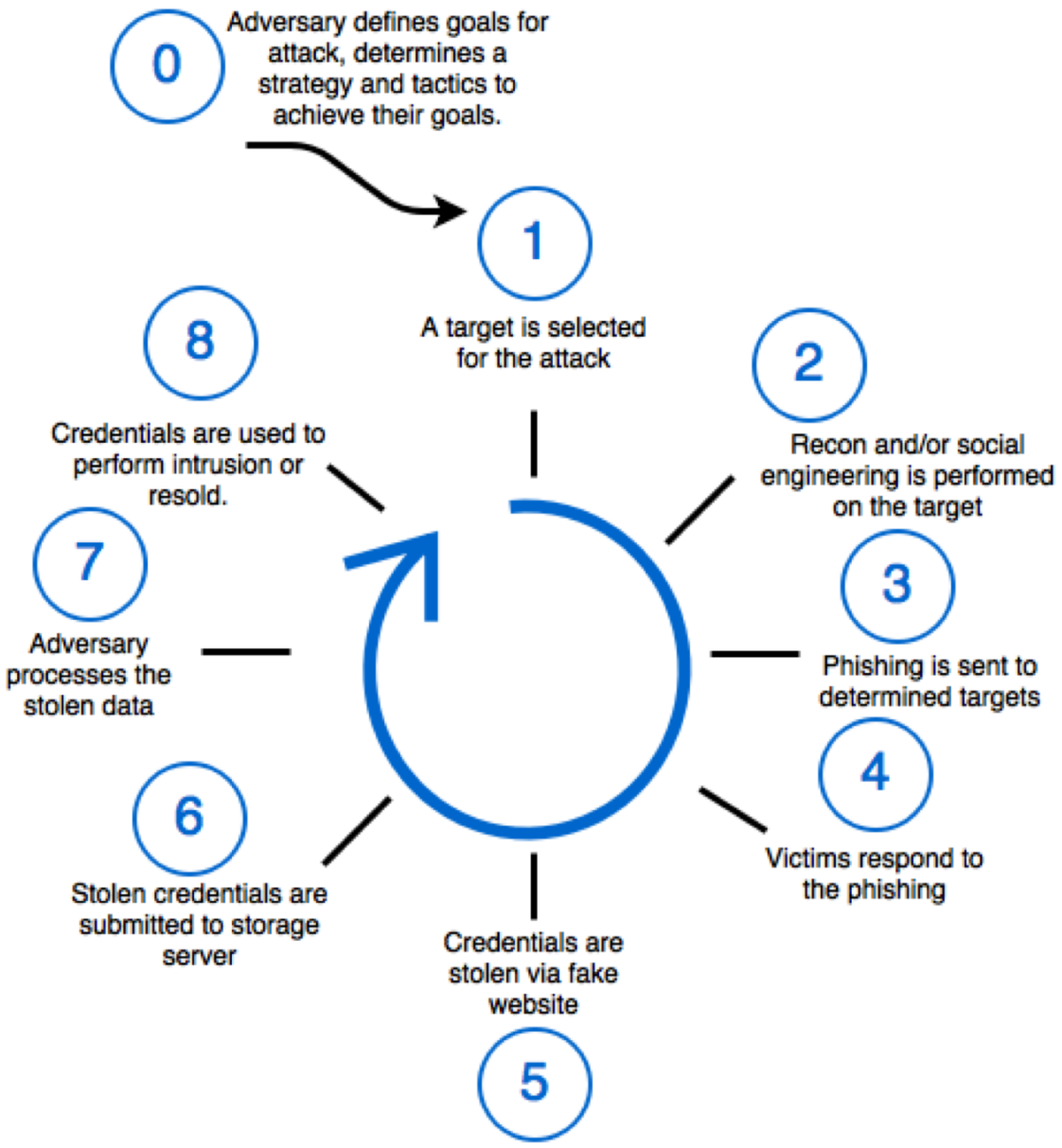
Procedure

A particular way of doing something, especially one that is characteristic or well-established



Let's talk procedures for a moment.

- Keep your purpose in mind
- Write actions down in the order they appear
- Gaps are okay and expected.
- Match the negative spaces to elements that can be inferred from inductive profiling.



An example of high level procedures that might be involved in a phishing attack.

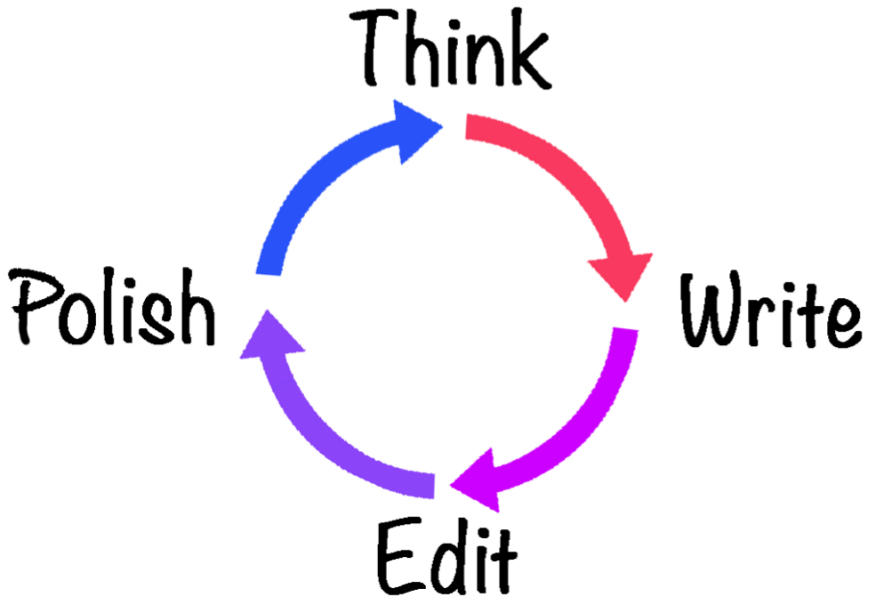
Spear Phishing

Vector: Attack
Mechanism: password reset, account closure, account verification/authorization
Medium: Email
Related Tactics: Phishing, Deception (Spoofing)
Associated Tactics: Clone, Whaling (BEC/CEO fraud), Cloud, Malicious Attachment
Overview
Spear phishing is a targeted attack on victims selected for a specific reason with tailored content.
Objective: Determined by the call to action and associated tactics employed.
Defining Characteristics
Phishing email with tailored content focused on a logical group of victims. This group is smaller than the full organization, which would be the focus of a shotgun blast. May come in waves. May contain links, attachments, directions or all the above.
Observable/Expected Elements

- **Pre-stage** [Defining Target, Recon]
  - Social engineering techniques (organization, individuals, geographic area)
  - Compromise of business associate or contractor (public, private, suspected)
  - Recon (access) of victim to gather information (scrape, solicitation, historical access)
  - Registration of mimicking (impersonating) domain
  - Duplicate content discovery (use of content, images, scripts)
  - Test drive of phishing (reputation sources, online archives or repositories)
  - Historical use (against same or other victims; see test drive)
- **Active** [Foothold, Lateral Movement]
  - Phishing email (by wave, burst)
  - Victim traffic to link in phishing email
  - Victim traffic to mimicked domain
  - Victim opens attachment (artifacts alerts, malware, decoys)
  - Malware presence (artifacts, alerts, lateral activity, persistence)
  - Malware downloads additional malware or tools (artifacts, alerts)
  - Traffic to rendezvous server (adversary's; to gather stolen data)
  - Reputation reporting (reputation source, open reporting, blacklist)
  - Malware reporting (as above)

Internal Observables

- Intelligence alert to public event (about victim or public news or relationship)
- Intelligence alert to private event (see public event)
- Intelligence alert (general, DNS re-use, pattern of activity noted)
- Blocking & Reporting (independent, phishing linked)

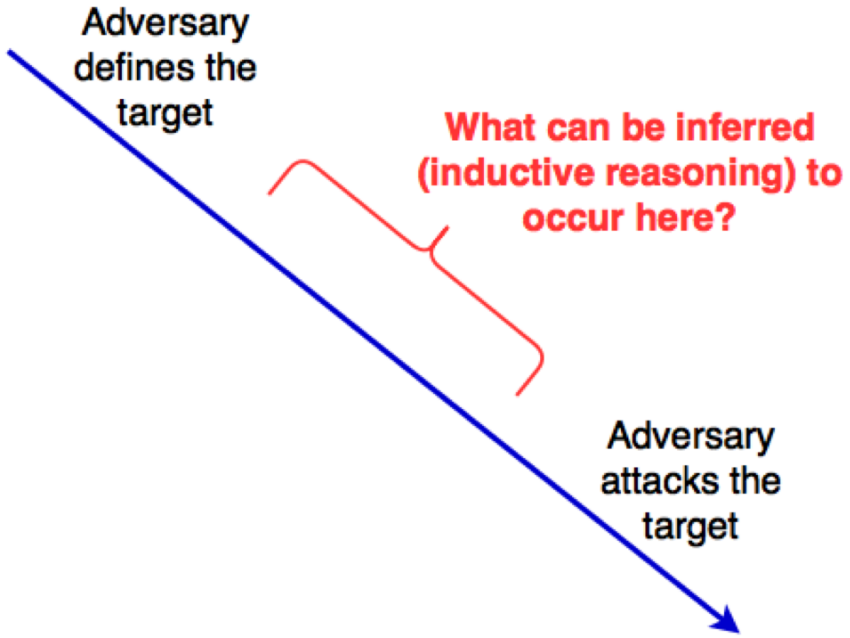


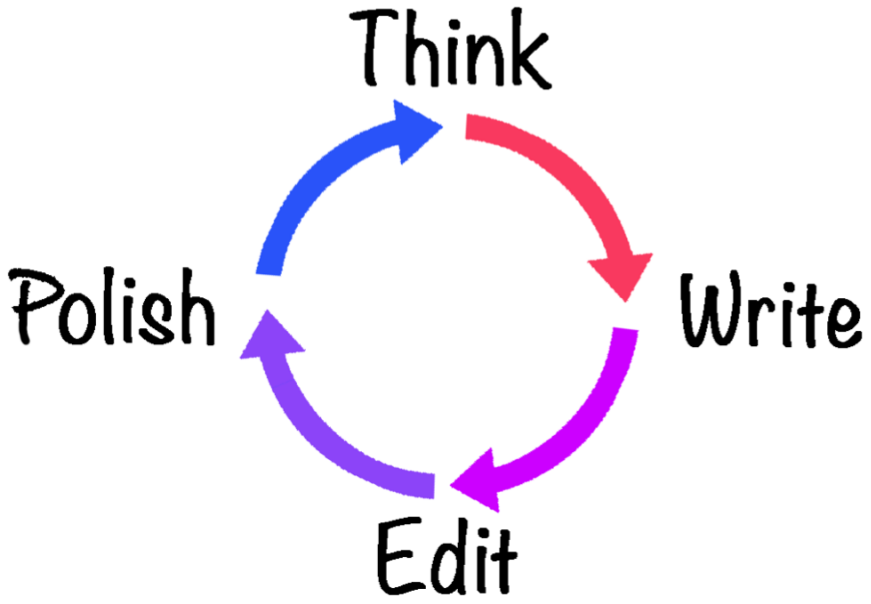
Workshop III - Characteristics File

Inductive Profiling (example)

What can be inferred to occur before an attack is launched?

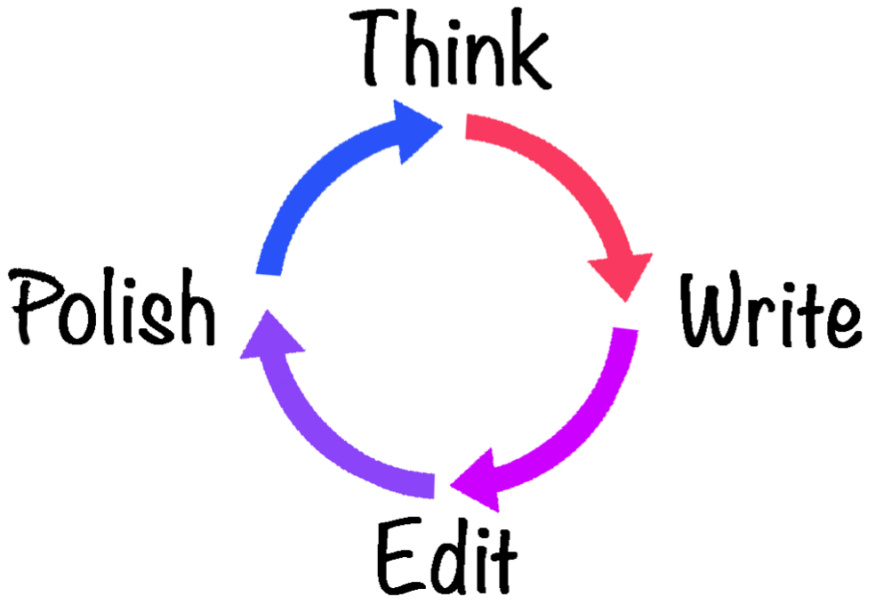
- Social engineering to gather personalized or specific information?
- Domain registration?
- Hosting for spoofed website?
- Cloning of a target website?
- Server to host the data?
- Setup for malware to download or append to phish?
- Purchase a phishing service to provide the desired result?





Workshop IV - Procedures

- Techniques are tools used to get immediate results. Think of them as a discrete action or task.
- Techniques begin to stand out when you collect enough procedures, since procedures are a series of ordered techniques.
- Techniques are individualized procedures that are unique to a person or group.
- Requires enough information to show the differences (deductive profiling) to discover.



Workshop V+ - Techniques

Files and Slides

https://github.com/CyberDefenses/Conventions

Questions?

Twitter: @montystjohn
LinkedIn: www.linkedin.com/in/monty-st-john-3842692
Github: github.com/corumir
CDI Github: github.com/cyberdefenses