IV. CYBER THREAT INTELLIGENCE

ibm.com/topics/threat-intelligence

Cyber Threat Intelligence (CTI)

detailed, actionable threat info for preventing & fighting cybersec threats targeting an org

* enables security teams to take effective, data-driven acts. to prevent cyberattks before they occur
  ↳ prevent biases by analysts in decision-making
* helps orgs. detect & respond to attks in progress faster

gca.isa.org/blog/what-is-cyber-threat-intelligence

Types

Strategic Intel.

* challenge: poor business & organizational decisions are made when adversary is misunderstood
* non-technical threat landscape info
  ie., info pertaining to intent, capability & timing of impending attks
  ↳ informs risk mgmt & organizational direction
* industry vertical; most often used by senior decision makers
* common srcs: media, gov. policy docs, industry reporting, open source

Tactical Intel ie., TTPs

* challenge: orgs often only focus on singular threats
* concentrates on specific threats & their immediate implications
  ↳ informs network level action & remediation
* supports day-to-day goals of security teams (ex., threat hunting, incident response, vuln. mgmt)

Operational Intel. ie., real-time monitoring

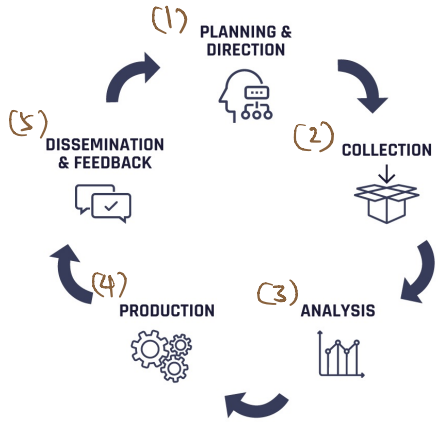
* challenge: threat actors favor techniques that are effective, opportunistic & low-risk
* work performed by threat hunters & incident responders perform to catalog adversary behavior, advise holistic remediation, & show examples of threat hunting processes

crowdstrike.com/cybersecurity-101/threat-intelligence

Characteristics of Good CTI

(1) actionable: provides info usable by security teams to address vulns., prioritize & remediate threats, eval. existing or new cybersec tools
(2) accuracy: success always outweighs errors & mistakes
(3) completeness: analyst must mine, research & otherwise provide all relevant info to detect threat in effort to prevent it
(4) context: covers → threats targeting org (contextual)
  ↳ threat actors who might carry out the attks
  ↳ TTPs used by threat actors
  ↳ IoCs that might signal a specific cyberattk
(5) reliability: maintains high credibility (in src & data credibility rating) — ref. [Admiralty Rating]
(6) relevance: focused on generalities (ex., lists of common malware strains), but on specific vulns. in org's attk surface, the attks they enable, & assets they expose (ie., must be pertinent to org)
(7) timeliness: corrective actions must be broadcast quickly & to large audiences to prevent further intrusions/ compromises

CTI Lifecycle



flashpoint.io/blog/threat-intelligence-lifecycle/

Key Objectives

(1) set scope & objectives for core intel roles & processes
(2) deploy data gathering & processing techniques & srcs
(3) translate raw intel into meaningful & taxonomized actors, events & attributes
(4) assess intel significance & severity based on business & environmental context
(5) report on finished intel, considering urgency & confidentiality

ACT: Authenticity, Competency, Trustworthiness

Admiralty Rating (a NATO system)

method for evaluating & rating collected intel

* impt data quality & src reliability assessment tool
* consists of 2-char notation that evaluates:

(1) src reliability
  (A) Reliable: Completely authentic w/ history of reliability, ACT
  (B) Usually Reliable: ∄ minor doubts in ACT, but ∃ a history of valid intel over a majority of time
  (C) Fairly Reliable: ∃ doubt in ACT. ∃ history of providing valid intel & data in the past
  (D) Not usually Reliable: Significant doubt regarding ACT. There has been valid data or info provided historically
  (E) Unreliable: Lacks ACT. History of providing invalid intel.
  (F) Cannot be judged: ✗ enough info to eval. src's reliability
(2) data credibility level
  (1) Confirmed: confirmed by other independent srcs; logical in itself; consistent w/ other info on subject
  (2) Probably True: ✗ confirmed; logical in itself; consistent w/ other info on subject
  (3) Possibly True: ✗ confirmed; reasonably logical in itself; agrees w/ some other info on subject
  (4) Doubtfully True: ✗ confirmed; possible but ✗ logical; ✗ other info on subject
  (5) Improbable: ✗ confirmed; ✗ logical in itself; contradicted by other info on the subject
  (6) Cannot be Judged: ✗ basis exists for evaluating validity of info

Traffic Light Protocol (TLP)

stdized sys. for classifying & handling sensitive info
↳ takes into acct: risk for privacy, reputation, or ops. (PRO) of orgs involved

TLP: RED Not for Disclosure
* for specific indv recipients only, ✗ further disclosure
* for when info ✗ be effectively acted upon wout significant risk for "PRO" of orgs involved

TLP: AMBER Limited Disclosure
* recipients can only spread info on a need-to-know basis w/in org & its clients
* for when info requires support to be effectively acted upon, yet carries risk to "PRO" of orgs involved

TLP: AMBER + STRICT
↳ restricts sharing to w/in org only

TLP: GREEN Community-Wide Disclosure
* recipients can spread info w/in their community, ✗ via publicly accessible channels
* for when info is useful to create awareness w/in wider community
* unless defined, "community" = cybersec \ defense community

TLP: CLEAR Unlimited Disclosure
* recipients hv ✗ limit to whom info can be disclosed
* for if info carries minimal to ✗ foreseeable risk of misuse (in accordance w/ applicable rules & procedures for public release)

Chatham House Rule

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

* If used effectively, this rule can help bring ppl together, break down barriers, generate ideas, & agree solutions

Should be defined by org's leadership when forming CTI

Intel Requirements

① Specific IR (SIR)
* detailed & specific questions or topics an org seeks to addr. thru their intel collection & analysis
  ex.: Do we have specific signatures to detect against exploitation of a certain vuln.? If not, can they be retrieved for somewhere?
* narrowly defined & can directly support decision-making
* formulated based on specific needs & priorities

② Priority IR (PIR) ($ SIR?)
* requirements that have greatest potential impact on org's mission & ops.
* focus resources on most impt intel need

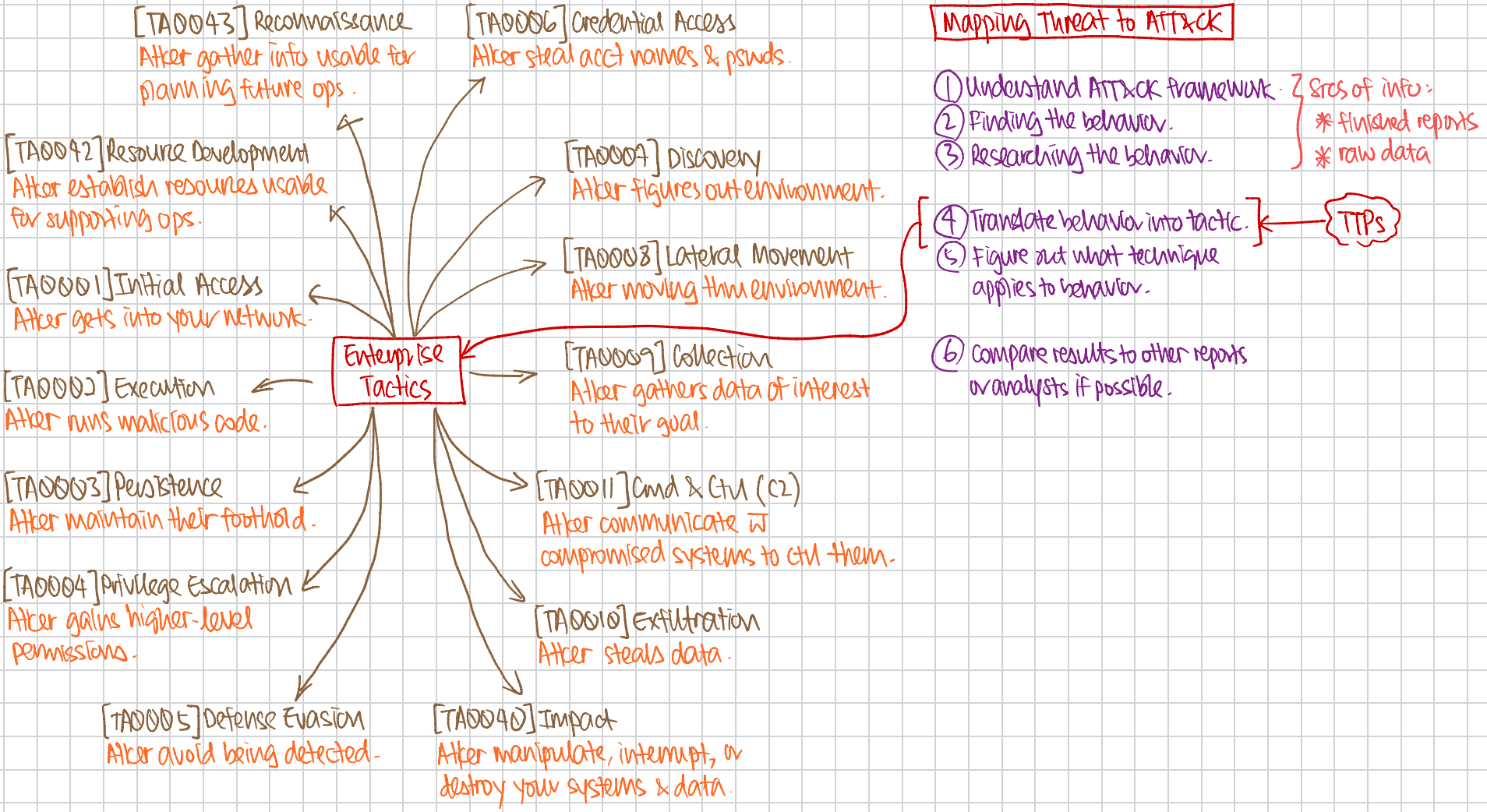
③ General IR (GIR)
* broader & less specific than SIRs & PIRs; they addr. general areas of interest
* essential for shaping overall intel collection & analysis effort
* helps provide context for understanding potential threats, emerging threats, or broader developments

CTI

Honeypots

decoy sys. resources set up to attract potential attkers
* designed to mimic real sys. \ services, but are also isolated or monitored
* primary goal: lure attkers into interacting w/ these sys. to observe & learn for their actions
* (purpose) a strategic component in cybersec;
  ↳ actively gather info abt potential threats & attkers (+)
  ↳ aimed to detect, deflect or study attempts at unauthorized use of infosys.
* objectives — early detection of cyber threats (+)
  — collecting valuable intel abt atk techniques
  — understanding potential vulns. w/in an org's network (+)
* types → research
  → high-interaction
    ↳ designed to get attkers to invest as much time as possible inside honeypot
    ↳ can observe how attkr goes abt looking for info, which info they prefer, & how they attempt to escalate access privileges
  → medium-interaction
    ↳ imitate elements of app. layer, but ✗ OS
    ↳ confuses \ stalls attkr to give orgs more time to decide how to ongoing atk
  → low-interaction
    ↳ less resource-intensive; gathers rudimentary info regarding kind of threat & where it came fr
    ↳ relatively simple to set up, makes use of TCP, IP & network services
    ↳ ∃ nothing inside honeypot to hold attkr's attn for considerable amt of time
  → production
  → virtual (VM honeypot)
  → hardware
* disadvantages
  ↳ attkrs who realize they fell victim to honeypot may retaliate
  ↳ honeypots require plenty of resources & expertise to set up properly (low ROI)
* real-world use cases:
  ↳ The Honeypot Project
  ↳ mapping CTI to ATT&CK

fortinet.com/resources/cyberglossary/what-is-honeypot
eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-honeypots-benefits-types/



Mapping Threat to ATT&CK

1. Understand ATT&CK framework.
2. Finding the behavior.
3. Researching the behavior.

Srcs of info:
* finished reports
* raw data

4. Translate behavior into tactic. ← TTPs
5. Figure out what technique applies to behavior.

6. Compare results to other reports or analysts if possible.