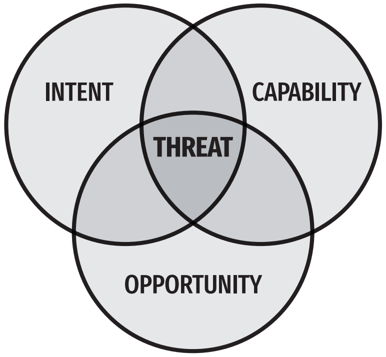
The Definition of a Threat

For a *threat* to exist to your organization, there must be an adversary with the intent, capability, and opportunity to target you.



Cognitive Biases and Logical Fallacies

A *cognitive bias* is a constraint on how analysts think that can influence incorrect decisions and assessments. Common biases include:

- **Anchoring—**Overvaluing one piece of information, often the first piece of information an analyst identifies
- **Confirmation bias—**The tendency to include or reject evidence based on its alignment to a preferred hypothesis
- **Hindsight bias—**The tendency to see an unpredictable event as an obvious result of a set of conditions or parameters. "I knew it all along."
- **Mirror imaging—**When we fool ourselves into believing that the entity/person/etc. that we are analyzing would behave in any way similar to what we would, given our experiences, biases, and life's context.

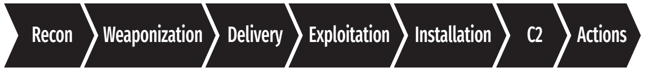
A *logical fallacy* is a flaw in reason. They often occur in conjunction with cognitive biases. Common fallacies include:

- **Argument from repetition—**Arguing so much that eventually people accept the conclusion to end it
- **Burden of proof—**Requiring someone to disprove someone else's claim instead of requiring proof
- **Cum hoc ergo propter hoc—**Correlation is not always causation

Frameworks and Models

The Lockheed Martin Cyber Kill Chain®

The Lockheed Martin Cyber Kill Chain is a model that outlines the seven stages of a cyberattack, from reconnaissance to exfiltration, helping organizations understand and disrupt adversaries' actions. It is best used for identifying and mitigating threats in structured, targeted attacks.



MITRE ATT&CK®

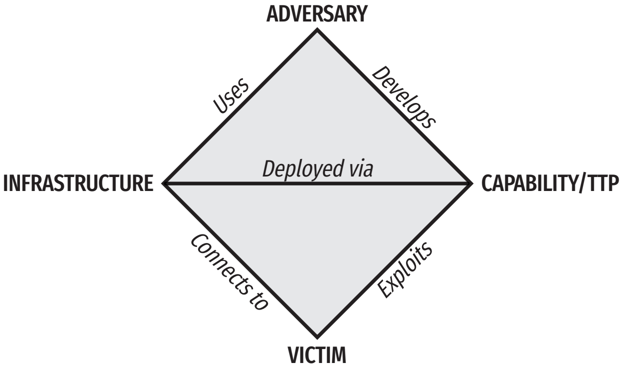
MITRE ATT&CK is a widely used framework that articulates adversary behaviors in tactics, techniques, and procedures. It's useful for mapping details of what adversaries do in a common language to more clearly communicate and compare.

ATT&CK enterprise tactics:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

The Diamond Model

The Diamond Model is a simple model that can guide cross-intrusion correlation and the creation of activity groups. To quote the authors of this model: "In its simplest form, the model describes that an adversary deploys a capability over some infrastructure against a victim."



SANS DFIR

CTI Cheat Sheet v1.0

This cheat sheet was created by Katie Nickels and Rebekah Brown, based on content from Robert M. Lee's FOR578: Cyber Threat Intelligence course. It is intended to be used as a reference for frameworks and concepts that are helpful for CTI analysts.

Requirements

Intelligence Requirements are objectives that analysts seek to satisfy through the intelligence process. They should:

- Ask only one question
- Focus on a specific fact, event, or activity
- Support a single decision
- Be available to the intelligence team and its consumers
- Only have a few priority intelligence requirements

Intelligence Requirement Examples

- **Strategic—**What business units are at most risk to cyber crime?
- **Operational—**What threat activity groups are currently active in our industry?
- **Tactical—**What indicators are most relevant to search for to quickly respond to the breach that has occurred today?

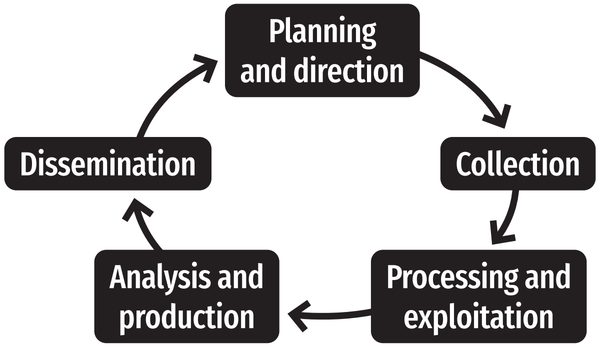
Useful Collection Sources

There are many collection sources that can be useful for CTI depending on requirements. Analysts should understand their collection on a technical level to determine what intelligence requirements they can satisfy. Consider using a Collection Management Framework to organize sources of data, what is available in the data, and how that data is processed and exploited. Regardless of the collection source, look for human fingerprints that indicate adversary choices.

Collection sources to consider include:

- **Malware—**hashes, header metadata, PDB strings, mutexes, import hashes. Look for human fingerprints like actor "handles," passwords, or IDs.
- **Network—**domains (actor-registered, legitimate but compromised, Dynamic DNS), IP addresses, ASNs, passive DNS resolutions, TLS certificates (hash values, dates valid on domains/IPs)

The Intelligence Life Cycle



Structured Analytic Techniques

Structured Analytic Techniques (SATs) are analyst approaches to better evaluate information while reducing the impact of bias.

Brainstorming should be used as a structured analytic technique to generate hypotheses or explore potential outcomes. It is especially useful in the early stages of analysis to encourage creativity, uncover hidden assumptions, and avoid groupthink.

Key Assumptions Check should be used when making critical decisions in analysis in order to identify and evaluate the assumptions underlying your judgments. It is valuable in situations where there is uncertainty or complexity to ensure the analysis is grounded, to uncover potential biases, and to assess whether the assumptions remain valid as new information emerges.

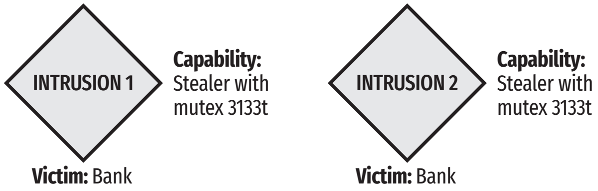
Analysis of Competing Hypotheses (ACH) should be used when evaluating multiple plausible explanations or outcomes for a complex problem where evidence may support or refute different possibilities. It is particularly effective in reducing cognitive bias, ensuring a systematic approach to analysis, and identifying the hypothesis that is most strongly supported by the available evidence.

Seven steps of ACH:

- Hypothesis
- Evidence
- Diagnostics
- Refinement
- Prioritization
- Sensitivity
- Conclusion and Evaluation

The Rule of 2

The Rule of 2 is a shortcut for creating activity groups. Look for consistency in multiple intrusions across two or more features of the Diamond Model.


INTRUSION 1
Capability: Stealer with mutex 3133t
Victim: Bank
INTRUSION 2
Capability: Stealer with mutex 3133t
Victim: Bank

Example: We create a new activity group called FUZZYSNUGGLYDUCK based on overlap in victim and capability. If we see a third intrusion that uses a stealer with mutex 3l33t that also targets a bank, we attribute that to the FUZZYSNUGGLYDUCK activity group.

Creating an Assessment

You can think of an assessment like an equation:

Assessment = Confidence + Analysis + Evidence + Sources

Example: I assess with **high confidence** that **ice cream will be served at break** based on **the freezer in the lobby** and **multiple SANS instructors** who have told me this will happen.

Consumption and Generation

Consuming cyber threat intelligence involves collecting, analyzing, and using information about threats to protect an organization.

Example: Reviewing an open source threat report to extract indicators of compromise that the SOC can use for detection.

Generating cyber threat intelligence involves analyzing, creating, and sharing actionable insights, such as analyzing attack patterns or identifying new threats, to inform others or improve collective defenses.

Example: Mapping intrusions to the Diamond Model to identify a new activity group targeting your organization and disseminate information about TTPs to inform detection.