**Feedback Phase**

You will see in different models of the CTI lifecycle the feedback phase might be presented differently. Sometimes it is lumped together with dissemination, when the emphasis is usually placed on getting immediate and real time feedback with your stakeholders.

Other times it is omitted all together, usually when the author is emphasizing that the CTI cycle is a complete circle and after dissemination your feedback should be backed into the "Planning and Direction" aspect of the lifecycle.

Believe both are valid interpretations of the model.

For the purposes of my project I separate this step out and have a different philosophy about this.

* Feedback is absolutely a step that should feed into your Planning and Direction step. CTI lifecycle truly is a "circle of intel" but it should not be mistaken as being the same step.
* Feedback cycle should be done continuously where Planning and Direction typically takes place during specific intervals. You should have a distinct process from collecting feedback about many products from many of your stakeholders, while your Planning and Direction steps should be done after an *accumulation* of that feedback. Otherwise you'll give your team whiplash reacting and changing direction from every piece of feedback you get.
* Feedback cycle in my particular CTI philosophy should also include an "After Action Report" type activity on a regular basis to identify key skills and knowledge that your work is calling for, doing a quick SWOT (strengths weaknesses opportunities threats) together as a team. This should translate into time set aside for analysts to seek training and research in those areas. Adversary teams take time to develop skills and research your company for attacks, you must allow your CTI teams to do the same. **For this reason training is part of the CTI feedback step in this project**. You will also find various CTI lifecycle specific trainings in other sections of this project.
* And of course, what would any feedback phase me without all important metrics! I will note this is my general philosophy towards metrics. Before you approach defining and designing metrics for your CTI function you should ask yourself these questions:
  + What question is this metrics trying to answer? Does the data we have actually answer that question?
  + What action will we take if this metric reaches a certain threshold? Have we defined that action and that threshold?
  + How valuable is this metric compared to the time it takes to produce it? Can this metric be automated to reduce that time?

My personal philosophy is that a metric is meaningless unless some action will be taken if it reaches a threshold or trends significantly in a direction. So for example, how many blocks of malicious domains at the firewall. Sure, this may seem like a "CTI metric" but let's put it through this test. **What question are we actually trying to answer with this metric?** How well the firewall works? without a a number to compare the results to, this "metric" is meaningless. Now if you were able to say our firewall blocked three times more activity than the average rate of blocked domains by other companies in our industry, *that* might tell a story. **What action will be take if this metric reaches and threshold (or trends)?** If I tell you that we blocked twice as many domains this month as last month what will we as an organization do differently? Probably nothing unless that trend was caused by a change we made, such as implementing a threat feed into the firewall block list. **How valuable is this metric compared to how much time it takes to produce?** Well maybe this is a super easy metric to automate, it takes only seconds to come up with. Ok it is low value, but maybe it fills space on a dashboard. However, if this metric had no decisions or actions an organization would take as a result of trends or certain thresholds, or if it is unclear what CTI question (ahem Intelligence Requirement or Priority Intelligence Requirement) it is answering... then it is a lousy metric.

**Definition:**

The feedback phase in the cyber threat intelligence (CTI) lifecycle is crucial for the iterative improvement and relevance of intelligence operations. It involves the collection and analysis of responses from intelligence consumers and stakeholders regarding the utility, accuracy, and impact of the intelligence provided. This phase ensures that the CTI efforts are aligned with the evolving needs and priorities of the organization. By incorporating feedback, analysts can refine their collection strategies, analytical processes, and dissemination practices to enhance the precision, timeliness, and contextual relevance of the intelligence. Furthermore, it fosters a culture of continuous learning and adaptation, enabling organizations to stay ahead in the dynamic and complex landscape of cyber threats. Effective feedback mechanisms contribute to the development of a more proactive and resilient cybersecurity posture, optimizing resource allocation and strategic decision-making in defense against advanced persistent threats (APTs) and other cyber adversaries.

**Feedback**

**Templates for Feedback**

* RFI Feedback
* Feedback on IRs, PIRs
* Ad-hoc Feedback tracking

**Metrics**

* [John’s 2024 CTI Summit Workshop Ideas on Metrics](https://twitter.com/_John_Doyle/status/1752341039212306666)
* [Gert Jan’s Metrics spreadsheet](https://github.com/gertjanbruggink/Metrics)

**Training Resources**

* [Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends (Part 1)](https://www.sans.org/blog/helping-cti-analysts-approach-and-report-on-emerging-technology-threats-and-trends/)
* [Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends (Part 2)](https://www.sans.org/blog/helping-cti-analysts-approach-and-report-on-emerging-technology-threats-and-trends-part-2/)
* [Katie Nickel's Blog on Getting Started in CTI](https://medium.com/katies-five-cents/faqs-on-getting-started-in-cyber-threat-intelligence-f567f267348e)
* [Katie Nickel’s Suggested CTI Self-study Plan](https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a)

**Competencies**

* [Cyber Threat Analyst Onboarding | Process Street](https://www.process.st/templates/cyber-threat-analyst-onboarding/)
* [Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends (Part 1)](https://www.sans.org/blog/helping-cti-analysts-approach-and-report-on-emerging-technology-threats-and-trends/)
* [Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends (Part 2)](https://www.sans.org/blog/helping-cti-analysts-approach-and-report-on-emerging-technology-threats-and-trends-part-2/)
* [Mandiant Cyber Threat Intelligence (CTI) Analyst Core Competencies Blog](https://www.mandiant.com/resources/blog/cti-analyst-core-competencies-framework)
* [Mandiant Cyber Threat Intelligence (CTI) Analyst Core Competencies (Direct Link)](https://www.mandiant.com/sites/default/files/2022-05/cti-analyst-core-competencies-framework-v1.pdf)
* [CSV Enumeration of Core Competencies and Job Mapping Using It](https://tinyurl.com/CTI-Core-Competencies)
* [Mapping FOR578 Coverage to the CTI Core Competencies Framework](https://www.sans.org/blog/mapping-sans-for578-coverage-to-the-mandiant-cti-core-competencies-framework/)

**Interviewing**

* [Breaking Into the CTI Field: Demystifying the Interview Process and Practice Interview Questions](https://medium.com/@Shinigami42/breaking-into-the-cti-field-demystifying-the-interview-process-and-practice-interview-questions-37cc8168f10c)
* [How Red Canary Recruits CTI Talent](https://redcanary.com/blog/cyber-threat-intelligence-hiring/)
* [What to Expect When Interviewing at Dragos](https://www.dragos.com/blog/what-to-expect-when-interviewing-at-dragos/)
* ["Intelligently Developing a Cyber Threat Analyst Workforce” SANS Podcast](https://www.sans.org/webcasts/intelligently-developing-a-cyber-threat-analyst-workforce/)

**Intrusion Analysis Practice**

* [Microsoft’s KC7](https://kc7cyber.com/)
* [KC7 GitHub](https://github.com/kkneomis/kc7)
* [KC7 Twitter](https://twitter.com/KC7cyber)
* [How to host your own KC7 CTF](https://docs.kc7cyber.com/)
* [KQL Cheatsheet 1](https://github.com/microsoft/Kusto-Query-Language/blob/master/doc/tutorial.md)
* [KQL Cheatsheet 2](https://techcommunity.microsoft.com/t5/azure-data-explorer-blog/azure-data-explorer-kql-cheat-sheets/ba-p/1057404)
* [Mining your SPAM folder to discover and analyze malicious content](https://alexandertasse.medium.com/junk-folder-analysis-for-dec-2023-490c51995f7a)

**TTP Mapping and Attribution**

* [SANS 2019 CTI Summit Presentation by Sarah Jones, “A Brief History of Attribution Mistakes”](https://www.youtube.com/watch?v=Y3EPkDUoGyc)
* [VERIS Threat Modeling Framework](https://veriscommunity.net/)
* [Mandiant’s Targeted Attack Lifecycle](https://www.mandiant.com/resources/targeted-attack-lifecycle)
* [The Cyber Kill Chain (Summary)](https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html)
* [Intel-driven Computer Network Defense (White Paper)](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf)
* [The Cyber Kill Chain (White Paper)](https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf)
* [The Diamond Model of Intrusion Analysis (White Paper)](https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf)
* [The Diamond Model of Intrusion Analysis (Slides)](https://digital-forensics.sans.org/summit-archives/cti_summit2014/The_Diamond_Model_for_Intrusion_Analysis_A_Primer_Andy_Pendergast.pdf)
* [ThreatConnect's Application of the Diamond Model to Star Wars](https://threatconnect.com/wp-content/uploads/Star-Wars-Slick-Sheet-1-1.pdf)
* [MITRE ATT&CK (Website)](https://threatconnect.com/wp-content/uploads/Star-Wars-Slick-Sheet-1-1.pdf)
* [MITRE ATT&CK (White Paper)](https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy)
* A 2020 [blog post](https://www.threatintel.academy/diamond-model-kill-chain-attack/) from Diamond Model author, Sergio Caltagirone, about combining the Diamond Model, Kill Chain, and MITRE ATT&CK
* [MITRE recorded training on how to use ATT&CK](https://attack.mitre.org/resources/training/cti/)
* [Cybrary course on understanding MITRE ATT&CK TTPs and mapping in Navigator](https://www.cybrary.it/course/application-of-the-mitre-attack-framework/) (old)
* [Cybrary course on applying MITRE ATT&CK to CTI](https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-cyber-threat-intelligence/) (old)
* [Newly updated MITRE ATT&CK (MAD) training platform](https://mad.mad20.io/)
* [Best Practices for MITRE ATT&CK Mapping](http://www.cisa.gov/sites/default/files/2023-01/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf)
* [Mitre's Threat Report ATT&CK Mapper (TRAM) Tool](https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/threat-report-attck-mapper-tram/)
* [CISA released MITRE ATT&CK Mapping tool, "Decider"](https://www.mitre.org/news-insights/news-release/cisa-releases-new-tool-mapping-adversary-behavior-mitre-attack)
* …[“Decider” Fact Sheet](https://www.cisa.gov/resources-tools/resources/decider-fact-sheet)
* …[”Decider” GitHub Repo](https://github.com/cisagov/decider)
* [NIST SP 800-53 Controls Mapping to MITRE ATT&CK](https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/nist-800-53-control-mappings/)

**Malware**

* [Limitations of Malware Analysis in CTI](https://www.dragos.com/wp-content/uploads/Threat-Intelligence-and-the-Limits-of-Malware-Analysis.pdf)
* [VirusTotal for Investigators](https://storage.googleapis.com/vt-gtm-wp-media/virustotal-for-investigators.pdf)
* [Censys’s blog on infrastructure pivoting](https://censys.com/a-beginners-guide-to-tracking-malware-infrastructure/)
* [VX Underground's APT Archive](https://vx-underground.org/APTs)
* [Objective See’s Mac Malware Archive](https://github.com/objective-see/Malware)
* [Malshare](https://malshare.com/)

**CTI Conferences**

* [PulseDive’s list of recommended CTI conferences](https://blog.pulsedive.com/the-biggest-best-cti-events/)
* [Cyberwarcon](https://www.cyberwarcon.com/) and [SLEUTHCON](https://www.cyberwarcon.com/brunchcon)
* [FIRST CTI Summit](https://www.first.org/events/symposium/berlin2022/)
* [LabsCon (SentinelOne hosted)](https://www.sentinelone.com/blog/labscon-security-research-in-real-time-talks-not-to-miss-part-one/)
* [PivotCon](https://pivotcon.org/)
* [VirusBulletin Conference](https://www.virusbulletin.com/conference/vb2022/)

**Books/TV Shows/Movies/Podcasts**

* Midway
* Cliff Stoll’s [Cuckoo’s Egg (.pdf)](http://bayrampasamakina.com/tr/pdf_stoll_4_1.pdf)
* Cliff Stoll’s [Cuckoo’s Egg (2017 CTI summit talk)](https://www.youtube.com/watch?v=1h7rLHNXio8)
* [Sandworm](https://www.penguin.com.au/books/sandworm-9780525564638) by Andy Greenberg
* Thomas Rid’s [Active Measures](https://www.amazon.com/Active-Measures-History-Disinformation-Political/dp/0374287260)
* [Thinking, Fast and Slow](https://www.amazon.com/Thinking-Fast-Slow-Daniel-Kahneman-ebook/dp/B00555X8OA)
* [The Thinker’s Toolkit](https://www.amazon.com/Thinkers-Toolkit-Powerful-Techniques-Problem/dp/0812928083)
* [Intelligence-Driven Incident Response: Outwitting the Adversary](https://www.amazon.com/Intelligence-Driven-Incident-Response-Outwitting-Adversary/dp/1491934948)
* [Visual Threat Intelligence: An Illustrated Guide For Threat Researchers](https://www.amazon.com/Visual-Threat-Intelligence-Illustrated-Researchers/dp/B0C7JCF8XD)
* [Splunk’s Bluenomicon](https://www.splunk.com/en_us/campaigns/bluenomicon-book-from-surge.html)