A Cyber Threat Intelligence Self-Study Plan: Part 1

medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a

Katie Nickels February 23, 2021

Katie Nickels

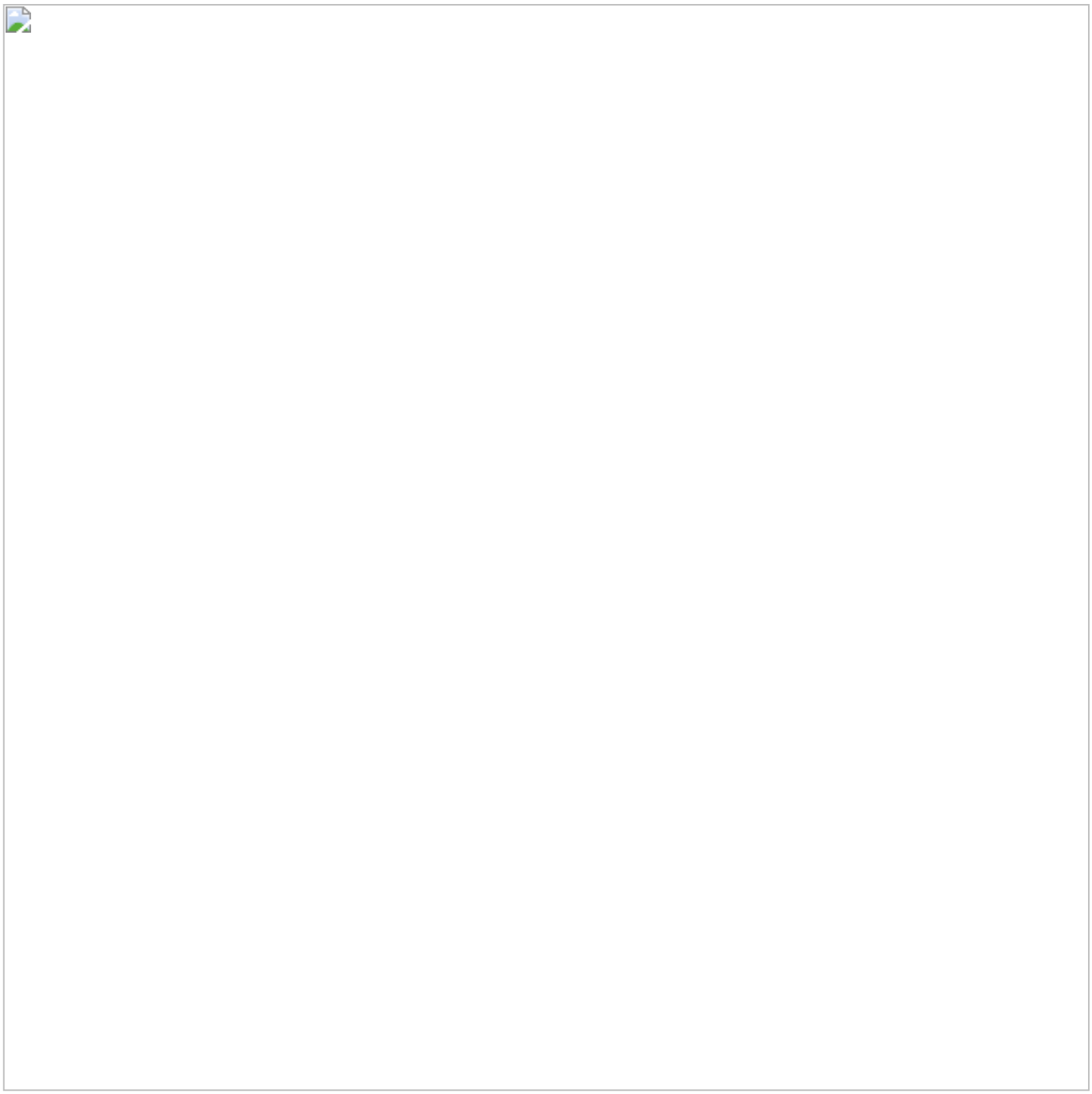
Feb 23, 2021

.

9 min read

There are many ways to learn. While some people prefer to have a live instructor in a course, others are great at doing self-study. I teach SANS FOR578: Cyber Threat Intelligence, which is a great course if you want to learn about cyber threat intelligence (CTI), but I realize not everyone can afford it.

Here's the good news: if you are committed, you can learn a lot of the same concepts that paid courses teach, but on your own. It won't be the same, but you can still learn a ton if this learning style works for you. I wanted to share a self-study plan to help out anyone who wants to take the initiative to learn about CTI. There are lots of great resources out there, but I realize as you're starting out that someone saying "go look at all the things!" isn't that helpful because you're not sure where to look. My goal is to bring together free resources I'd recommend studying and provide a minimal framework and question to help tackle them.



My bookshelf! (in part…)

How to use this plan

Honestly, however it helps you! :) I wrote this with the idea that someone wanting to learn about CTI could work through it section-by-section, since some concepts build on each other. Be forewarned, if you do this entire thing, it's going to take a lot of time and effort! I've included resources to read and watch, things to do, and questions to think about, as well as a few optional paid resources if you want more. (Please note that some of the links directly download a PDF.) Maybe you work through this in order, but maybe you just need to learn more on specific sections. I highly recommend taking notes as you go as a way to reinforce the material and hold yourself accountable for thinking through and answering the questions—the critical

thinking is key to all of this. To be a good CTI analyst, you can't just consume something, you have to think about what you think of it and how you can apply it. Consider how you want to organize your notes before you start (a notebook, a binder with dividers, Google Docs, OneNote, or whatever else works for you).

If you're new to this industry, I recommend finding someone to help you out as you have questions. As much as I wish I could, I don't have the energy to do this myself, BUT here's my offer — if you tag me in a tweet (@likethecoins) that explains why you want to go through this self-study and why you need a mentor, I would be happy to re-tweet that for you to try to connect you with someone in the community who can help. I'm lucky to have many CTI friends who are passionate about helping newer people in this industry.

I'll be breaking this plan up as I have time to write each section. I haven't completely decided on topics for future sections, but here are a couple I plan to include: tools/TIPs, pivoting, open source research, evaluating reports, clustering, indicators/TTPs, threat modeling, assessments/uncertainty, and dissemination/writing.

Part 1 topics include:

- Intelligence
- Cyber Threat Intelligence
- Requirements
- The CTI Community
- Frameworks and Models

Intelligence

CTI represents the convergence of two communities: intelligence and cybersecurity. Good CTI analysts will understand fundamentals about intelligence and bring those principles to their work. Sometimes I've seen analysts struggle to bring together "traditional intelligence" and cybersecurity concepts, so I recommend doing this section first, and being relentless about considering how it applies to everything that follows.

Read and watch

- Read about the 9 principles of , starting with "1. Focus on Policymaker Concerns" on page 9 (you can skim the rest). Sherman Kent is a figure you should know about, and these principles of his analytic doctrine are core to what I think an intelligence analyst should be.
- Read Richards Heuer's . This is a great intro to several important principles about how we think as intel analysts — including cognitive biases and structured analytic techniques.
- Read about the .

Things to do

- Go research Sherman Kent and Richards Heuer — why were they considered important in this field (especially in Western intelligence)? Who are other figures that are important in intelligence, especially from a -Western perspective? (go research and find at least one)
- Scroll around and go research cognitive biases to find a few that weren't in Heuer's book.
- Identify your own cognitive biases in everyday life. This is HARD, but you can do it if you're honest with yourself. Tip: anything that makes you angry is a great place to look for biases. Write down your cognitive biases when you find them.

Questions to think about

- Why do intelligence analysts consider Sherman Kent's analytic doctrine to be so important? What would happen in situations where analysts did not follow these principles? Think of examples for each principle. Can you think of situations you've seen — whether in intelligence or elsewhere — where people have not followed these principles? What happened?
- As you go through the rest of this self-study, when do you see analysts adhering to Kent's analytic doctrine? When do you see them NOT adhering to it? What is the result?
- Why does the intelligence cycle exist? What makes intelligence different from raw data?

Optional paid resource

> If you're looking to learn more about the US Intelligence Community, I recommend Mark Lowenthal's "Intelligence: From Secrets to Policy". Older editions are almost as good and are much cheaper. This is the book I was assigned in my intelligence class in grad school and it's widely used in higher education.

Cyber Threat Intelligence

This section is meant to introduce you to some fundamental concepts in CTI and learn a little about its history.

Read and watch

- Watch I did.
- Read from Sergio Caltagirone. Don't get hung up on the ICS-specific terms (you can skim those parts if you want); think of them as examples of CTI…the point of you reading this isn't to become an ICS expert, it's to learn some fundamental principles of CTI.
- Watch of Chris Sanders' free Cuckoo's Egg course. (At some point, I recommend working through the whole thing because it's an amazing free resource from Chris, but for CTI, week 6 is key.) This course covers a lot of the topics below too.
- If you're setting up a team/CTI program, watch this I did with Jackie Abrams of DomainTools. You need a (free) SANS account to log in, then register so you can view the recording. I also recommend reading , especially if you're setting up a team.

- Read a key report in CTI history: the from 2013.

Things to do

- Go find a few different definitions of CTI. How are the definitions different? Which one resonates most with you? What is the earliest date you can find the term “cyber threat intelligence” used?
- Research where the term “Advanced Persistent Threat” came from. Go research news around the APT1 report — why was that so important?
- Research and take a few notes on at least one major CTI event or intrusion you can find prior to 2013 (when the APT1 report came out). (If you need a place to get started check out) What was noteworthy about the event/intrusion you chose? Can you find any similar events/intrusions (for example, involving similar actors or TTPs) that occurred after it?

Questions to think about

- What principles do you see from the intelligence section that you see also apply to CTI? How do you think CTI is the same or different from traditional intelligence?
- How long has CTI been around as a discipline? As you go through this curriculum, think about who you see as key people and organizations who have driven the development of CTI.
- How does the traditional intelligence cycle translate to CTI?

Optional paid resources

- If you’re looking for a good book on CTI, I highly recommend Rebekah Brown and Scott Roberts’ .
- If you’re looking for paid CTI courses, I recommend (full disclosure: I teach it!), Joe Slowik’s , or any of . is more forensics-based, but the principles he teaches are key to those you should develop as a CTI analyst.

Requirements

These are so important that they get their own section, though some of this content is covered in the above CTI section.

Read and watch

- Read Scott Roberts’ on requirements.
- Watch Andreas Sfakianakis’ .
- Read Pasquale Stirparo’s .

Things to do

Choose a CTI team at an organization— you can imagine one or use a real one you know of (if you're trying to get a CTI job at a company, choosing that org would be great for this exercise). Write down strategic, operational, and tactical intelligence requirements you think that they might have based on your research (or made-up information) about that company.

Questions to think about

Why are requirements so important in CTI? What do you think would happen if a team did not have requirements?

The CTI Community

If you want to get involved in CTI, it's important to get to know the community, including key people and stakeholders. Like anything in life, everyone has different perspectives, backgrounds, and motivations. You should get to know people in the community, while also realizing that we all have our own cognitive biases (see how this builds on earlier material?), so you should always think critically about the perspectives someone presents — and whether you agree or disagree (always doing so respectfully without resorting to ad hominem attacks).

Things to do

- Create a Twitter account (it doesn't have to be in your real name) and go find people to find in CTI to follow. If you're not sure who to follow, check out me (@likethecoins) and see who I re-tweet and interact with, or follow some people I mention in this post. From your Twitter research, figure out what hash tags the CTI community uses. Follow these hash tags — you might find it easier to use to do this.
- Create an RSS feed of some resources you see those Twitter accounts share. You could use Feedly's free offerings to do this, or many . Building a good RSS feed is essential for many CTI roles, as it will allow you to stay up to date with new blog posts and reports. Remember that your RSS feed will grow and change over time based on new sources you find and your needs (requirements!!!), so don't worry about getting it "perfect" to start.

Questions to think about

- What people and companies make up the "CTI community"? (For example, vendors are one group— what are others?) How does the "CTI community" overlap with other parts of the cybersecurity community like DFIR?
- What roles do CTI analysts and CTI companies play in the community? What are their backgrounds and what do they do? Do they have a specific angle or agenda? What role does media play in the CTI community?
- What are analysts discussing about CTI on Twitter? Who seems to represent what perspectives? What in their background might lead them to have those perspectives?

- What are key events and conferences that happen in the CTI community? Which are free and how much do they cost? What approach/angle do different events take?

Frameworks and Models

The “big three” frameworks and models I recommend you know about are the Cyber Kill Chain, the Diamond Model, and MITRE ATT&CK(R), though there are several others as well. It’s important for CTI analysts to understand what these are and how they can be applied, as well as what to be cautious of when applying them. Concepts from these frameworks and models will also be sprinkled throughout this self-study plan.

Read and watch

- Read Chris Sanders’ .
- Read the Lockheed Martin Cyber Kill Chain(R) .
- If you’re a Star Wars fan, read this on applying Star Wars to the Diamond Model. (If you’re not a fan, you can obviously still read it, it just might not make as much sense to you!)
- Read the . It’s dense, but it’s awesome, so break it up into parts if you need to.
- Click around the and skim various sections — maybe the “Quick Start” section or whatever section helps you learn what VERIS is and why you might use it.

Things to do

- Take the I created with my former teammate Adam Pennington, designed to take about four hours. (Note that it’s based on a previous version of ATT&CK, but you’ll still get the key points.)
- Find at least one example of a team (perhaps a cybersecurity vendor) applying each of the frameworks or models you learned about above. Think about your opinion of the pros and cons of how they applied it.
- Go look for examples of combining two or more of these frameworks. (Hint: Palo Alto’s Unit 42 team has a good one, though there are others!)

Questions to think about

- Why do CTI analysts use frameworks and models? When would each of these frameworks or models be useful?
- What are the limitations of frameworks and models? What are the risks of using them?

The end

I hope you found this first part of the self-study plan useful! If you have requests for topics you’d like to see most, let me know and I can use that to help prioritize what I work on next.