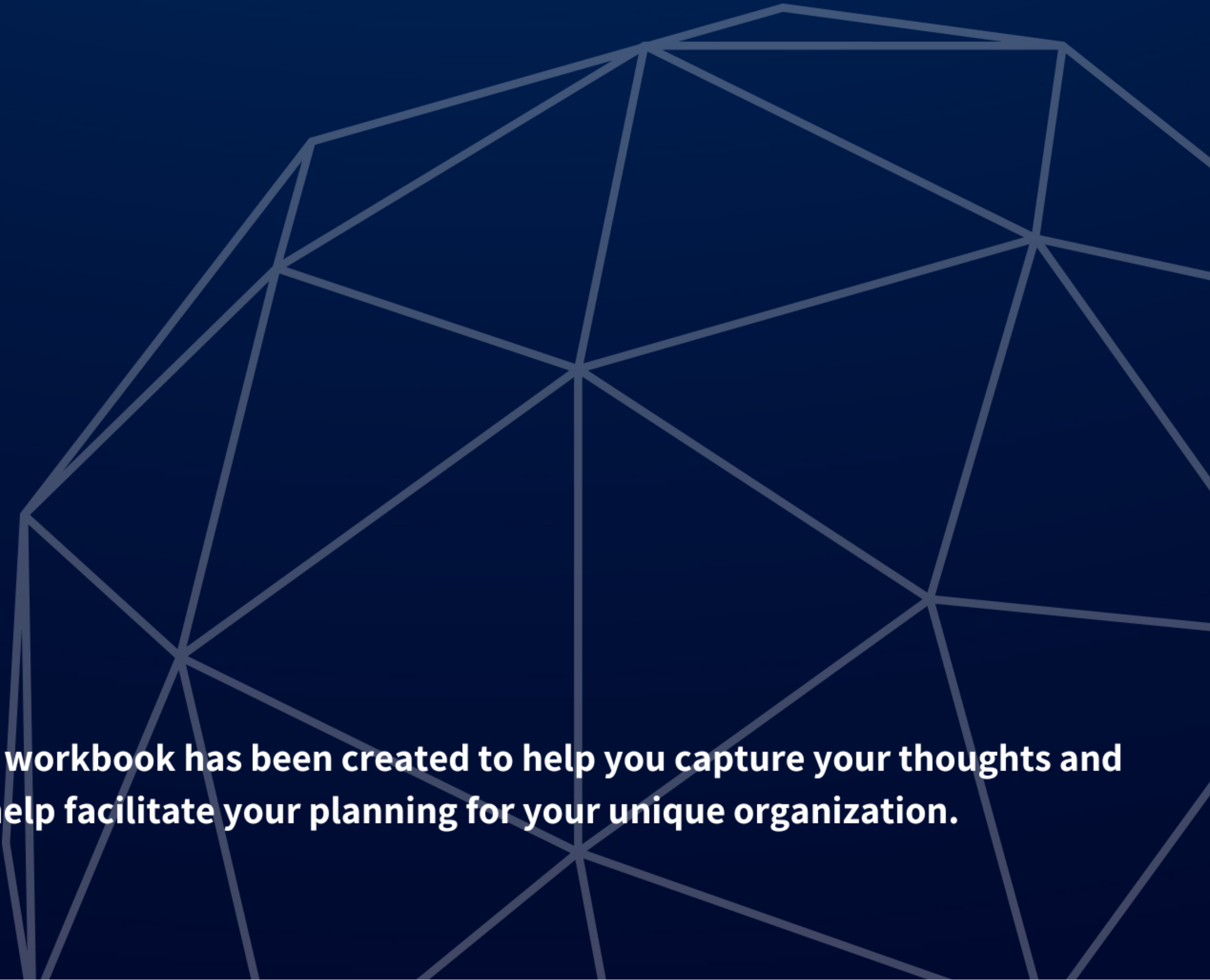
NISOS

Building a Cyber Threat Intelligence Program

Post-Workshop Workbook



Note: This workbook has been created to help you capture your thoughts and help facilitate your planning for your unique organization.

Table of Contents

1. Creating Consumers of Intelligence

A. Take an Educational Approach

When building a Cyber Threat Intelligence Program, it's important to make a conscious decision to spend the time and effort to have the tools you need to educate your various internal customers.

Questions to Get You Started

1. What are 2 ways that you're currently employing an educational approach to building consumers of intelligence within your organization?

Answer:

2. Who are your internal champions and how can you help them help you educate other internal customers?

Answer:

3. What personal or organizational blockers do you have for getting the time to educate your consumers?

Answer:

4. What are the tools/technologies you think you need to be effective in educating/informing your consumers?

Answer:

5. What tools/technologies do you already have that can be used to communicate your educational content?

Answer:

B. Create Internal Collateral

There are multiple ways to spread awareness, which is crucial to your success. The following are recommendations and ideas for how you can start to develop the types of content that will be easily consumed by your internal customers. Remember, you want to define your program and what it contains in a way that is easy to present. Short-form content around your capabilities or your data sources that contain the key points for the respective audience is helpful. And remember, it's helpful to maintain an internal team site that explains what your team does, provides resources, and explains how customers can engage with your team.

Questions to Get You Started

1. Who on your team can help you consolidate and prioritize your curriculum?

Answer:

2. Which of the following "tools" do you have at your disposal to help you disseminate education?

- □ Powerpoint Presentations
- □ Learning Management System
- □ Internal Slack Channel
- □ All-Hands Meetings
- □ Internal Marketing Resource
- □ Intranet Postings
- □ Create 1-pagers and reference sheets
- □ Email Communications
- □ Create Short Video Content
- □ Offer "office hours" to people to engage with you

C. Have Open Discussions to Baseline Your Internal Customers

We recommend that you talk about what intelligence is and isn’t - raw data vs intelligence. There is a spectrum of actionability that you should openly discuss with your leadership and internal customers. Whether it's during the *planning process* when you're getting started, *onboarding* new internal customers, or when doing a *periodic assessment* of your program. Come prepared to those discussions with any examples or success stories that you may already have had to help folks relate to the concepts. The following are some things you should think about ***before*** you set your meetings with internal customers:

Questions to Get You Started

You may **ask yourself** these questions ***before*** meeting with your internal customer(s):

1. What concepts are important for this customer to understand in order for them to effectively leverage your intelligence deliverables?

Your thoughts:

2. Where does this customer fall on the spectrum of actionability? Would they benefit from both situational awareness and direct action, or do they have higher priority use cases focused on tangible outcomes?

Your thoughts:

3. Will they be receiving finished intelligence or be working directly with the data sources or raw data collected?

Your thoughts:

4. For this particular internal customer, what examples or success stories have you already had that you can reference as examples of intelligence having a positive impact?

Your thoughts:

Questions to Get You Started

Questions you could ask your **internal customers**:

Advice: Capture this feedback in a manner that will allow you to reference it over time, not simply be collected and archived.

1. What do you think of when you hear the term “intelligence”? How do you see that relating to our organization?
2. Have you ever read an article online that helped you in your business-as-usual workflows? What was the article about?
3. What type of threats are top of mind for you?
4. What type of information about these threats would be helpful?
5. How would that information be helpful?
6. What type of decisions would it influence?
7. What stakeholders and teams are involved in those decisions?
8. Where do they fall on the spectrum of actionability?

Spectrum of Actionability

D. Gain Insights to Create Good Consumers of Intelligence

Be observant and purposeful in the discussions so that your consumers feel like they've been heard and their opinions matter. Not everyone will be a perfect consumer of intelligence after one discussion. It helps if you make notes of where your customer is at and any opportunities that may be good intelligence use cases to help bridge their gap of understanding. For some consumers, you may need to be more prescriptive with recommendations to ensure the intelligence is actionable where others may simply need data collected for them.

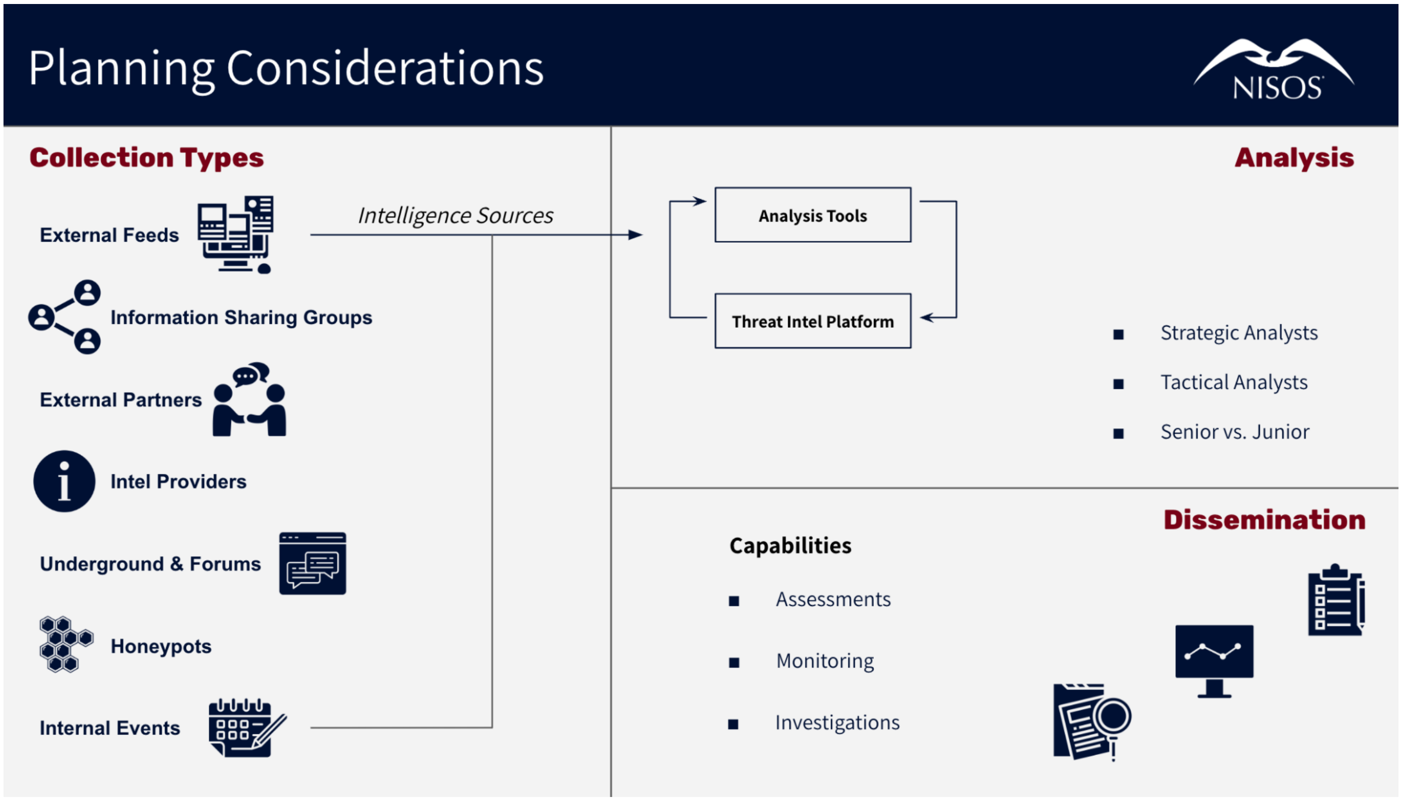
Questions to Get You Started

A list of things to be on a treasure hunt for may include:

1. Does the customer understand the difference between situational awareness and immediate action?
2. Were they able to provide examples of how they would use intelligence or the type of intelligence they would find helpful? If not, do you think if you provide them with examples it would help advance their understanding of the relevant concepts?
3. Where do they sit between complacency and paranoia? Are they unconcerned about threats facing them or are their perceptions of threats unrealistic?
4. What security controls are they responsible for? Would reporting on attacks or breaches of other organizations where the respective control was either ineffective or would have prevented the outcome resonate with them?

2. Planning Considerations

There are multiple ways to approach structuring your program to get leadership buy in and budget approval. Find what resonates and go with it.



Planning Considerations

NISOS

Collection Types

- External Feeds
- Information Sharing Groups
- External Partners
- Intel Providers
- Underground & Forums
- Honeypots
- Internal Events

Intelligence Sources

Analysis Tools

Threat Intel Platform

Analysis

- Strategic Analysts
- Tactical Analysts
- Senior vs. Junior

Dissemination

Capabilities

- Assessments
- Monitoring
- Investigations

Questions to Get You Started

You may **ask yourself** these questions to help you identify what areas resonate with leadership.

1. Are they more focused on the tools and data sources? If so, what are your gaps in collections or the data sources you have currently?

Your thoughts:

2. Are they outcomes or objective focused? If so, what is the final deliverable? What data sources do you need and how much analysis will be required?

Your thoughts:

3. Are they capabilities or security control focused?
   - Is it clear what the top priority is?
   - What data sources are required, analysis resources needed, and what do the final deliverables look like and provide?

Your thoughts:

A. Plan to Persevere

Remember, your first decision isn't final and isn't wrong if it helps get you the resources you need.

Questions to Get You Started

You may **ask yourself** these questions to reflect and plan:

1. What wasn't the perfect solution but gave you beneficial insights and opportunities?

Answer:

2. What is one thing you could tell your leadership you did to “make the best” of an unideal resource and how could you pivot that story with (If I had Y instead of X, Z would be possible).

Answer:

3. What is good about your current data sources and analysis resources? What would be better? What would be best?

Answer:

4. When does your budget planning start?

Answer:

5. When does business and performance goal planning start?

Answer:

6. Do they happen together or do you need to account for the difference in your planning?

Answer:

B. Revisit Your Wins and Where You Need Help

Each year is an opportunity to reevaluate your program, you may start simple and add (data sets, capabilities, analysts) as you go.

Questions to Get You Started

Do you have new customers or consumers who may be starting new with your intelligence deliverables?	☐ Yes	☐ No
Has leaderships' focus or priorities changed?	☐ Yes	☐ No
Has their understanding of how to leverage intelligence changed?	☐ Yes	☐ No
If tool focused, is there enough understanding of intelligence to shift planning to a capabilities or intel cycle focus?	☐ Yes	☐ No
Do you want to add a new deliverable next year?	☐ Yes	☐ No
Or a new data source?	☐ Yes	☐ No
Or Analyst resource?	☐ Yes	☐ No

C. Establish a Strong, but Flexible Framework

Your planning framework is the foundation for future metrics and KPIs.

Questions to Get You Started

Are you actively monitoring or detecting threats that can be categorized and quantified?	☐ Yes	☐ No
Are your data sources organized so that you can report on coverage across areas of the Internet?	☐ Yes	☐ No
Do you have a feedback loop for your intelligence deliverables, such as a customer survey, to help capture positive outcomes or feedback for qualitative measurements?	☐ Yes	☐ No
Do you have regular deliverables such as daily briefings or reports that can be measured quantitatively and also qualitatively with a feedback loop?	☐ Yes	☐ No

3. Managing Expectations

When engaging multiple levels of stakeholders, it can be helpful to understand what priorities they have so that you can align your goals with their goals. Here are some ways to approach different audiences:

A. Managing Expectations Upwards

It can seem daunting and intimidating to manage upwards. "Telling" leadership how intelligence works is not an effective way to manage upwards. Understand where they are starting from in regards to their expectation of intelligence and what problems they are hoping to solve with adding a CTI capability. Then, present and discuss your program using the planning considerations you think most closely align to where they are. Take the time to work to expand their knowledge of other aspects of your program that you think are critical for them to understand in order to take the next step. It can help your position if you present your recommendation as a question. For example: "Hey ________, would you mind if ________." or "My recommendation is _____________, how does that sound to you?"

Questions to Get You Started

You may **ask yourself** these questions to reflect and plan:

1. What is your leaderships' current perspective on intelligence?

Your thoughts:

2. Does it align with yours?

Your thoughts:

3. If not, what are the concepts that would help create better alignment?

Your thoughts:

4. Are there data sources or capabilities that leadership would benefit from knowing more about how they work?

Your thoughts:

5. Does providing examples of finished intelligence help their understanding of intelligence?

Your thoughts:

B. Managing Expectations Downwards

Having a well defined intelligence program is important for managing upwards, but it's almost more important for managing downwards to your team. Misalignment with peer teams who either make requests of your team or are accessing the data sources directly that results in follow-on questions or complaints about the data can burn out your team. This heightens the risk of team dissatisfaction and can contribute to talent retention issues. Spend the time up front to help your team understand what the program is and isn't.

Questions to Get You Started

You may **ask yourself** these questions to reflect and plan:

1. Does your team know what type of intelligence is their responsibility? Strategic, operational, or tactical?

Your thoughts:

2. Are there inbound requests that are not directly related to the team's objectives or performance goals?

Your thoughts:

3. Are deliverables and customer expectations clearly defined?

Your thoughts:

C. Managing Expectations Across the Organization

Don’t forget to work with your internal customers and peer teams. It can be helpful to have an educational type onboarding process when first bringing new internal customers onto your team's services. Share your program outline and structure with your peer leaders and teams. Prioritize having discussions around what they believe intelligence is and work with them to understand your objectives and capabilities.

Questions to Get You Started

You may **ask yourself** these questions to reflect and plan:

1. Are there any customers or peer teams that have unrealistic expectations of intelligence currently? Did they go through an onboarding process?
2. Are there concepts that would be beneficial to go over with them?
3. Would it help to educate them on how the data sources work and their limitations?
4. Do you have a feedback loop to help with making adjustments to ensure ongoing delivery of intelligence meets their expectations?