



WORKBOOK



The 30 Day CTI Decision-Speed Workbook

A step-by-step plan
for threat intelligence teams

How to use this workbook

This workbook is a companion to your CTI Decision-Speed Assessment. The guide helps you understand where you are. This workbook helps you make one clear step forward in the next 30 days.

You will:

- ✓ Focus on a small number of high value workflows
- ✓ Improve the path from “new signal” to “clear decision”
- ✓ Reduce manual busywork
- ✓ Start to standardize where high risk investigations happen, so analysts can move faster without adding risk

You can run this as a solo project or with a small working group from CTI, SOC, and one business stakeholder.

Recommended cadence:

- **Week 0:** choose scope (30 to 60 minutes)
- **Weekly session:** 60 to 90 minutes
- **Light async work:** in between
- **End of week 4:** 60 minute review

WEEK 0

Choose your focus

Before you start Week 1, pick a single workflow and capture a quick baseline.

Step 1: Capture your starting point

Use the self assessment from the main guide. Write your total maturity score here:

→ Total maturity score: _____

→ One sentence on how CTI feels today: _____

Example prompts:

→ How CTI works today in practice: _____

→ What bothers us the most about it: _____

Step 2: Choose one primary workflow

Select one workflow where better decision-speed will clearly matter in the next 30 to 60 days. For example:

- ☐ Breaking threats against your core infrastructure
- ☐ High priority vulnerabilities in your main product
- ☐ Vendor evaluation for a new critical SaaS provider
- ☐ Regional market expansion or new data residency requirement

Primary workflow for this 30 day experiment

Stakeholders for this workflow:

→ CTI owner: _____

→ Operational owner (SOC, vulnerability, fraud, etc.): _____

→ Business owner (if any): _____

This is where you will apply each weekly exercise.

WEEK 1

Map your threat landscape to your business context

★ **GOAL:**

Focus your attention on the threats that can actually hurt the workflow you chose.

🕒 **TIME REQUIRED:**

4 to 6 hours total

👤 **OWNER:**

CTI lead or senior analyst

Action 1: Identify your crown jewels for this workflow

Ask: If this workflow fails badly, what hurts the most?

Examples:

- Customer data stores behind a customer portal
- Payment and billing systems
- Identity provider and single sign on
- Core data stores that hold regulated or sensitive data
- Key partner or supplier integrations

List 3 to 5 items:

1.

2.

3.

4.

5.

Action 2: Map relevant threats to those assets

For each crown jewel, list the threats that really matter. Use sector, technology stack, geography, and recent incidents as guides.

Prompt questions:

- Which threat actors or campaigns have targeted similar assets
- Which techniques are most realistic for our environment
- Which third parties or vendors could become stepping stones

Fill in a table:

CROWN JEWEL	RELEVANT THREATS OR CAMPAIGNS	NOTES ON LIKELIHOOD OR IMPACT

Action 3: Note where high risk investigations happen today

For this workflow, ask:

→

Where do analysts open suspicious links, documents, or tools

→

Are they using improvised virtual machines or standard workstations

→

Do they have access to a safe, isolated environment for malware and infrastructure research

Current state (check all that apply):

☐

Secure analysis environment or sandbox

☐

Defined lab network

☐

Ad hoc virtual machines

☐

Regular corporate workstations

☐

Other: _____

This sets you up for later weeks when you standardize environments.

Action 4: Prioritize threats by likelihood and impact

Review your table and mark each threat with **L for higher likelihood** or **H for higher impact**. Circle or highlight the top 5 to 10 threats where CTI can make the biggest difference for this workflow.

Week 1 Deliverable

Create a one page “Threat Landscape Overview” for this workflow that includes:

- ✓ The crown jewels in scope
- ✓ The top 5 to 10 relevant threats or campaigns
- ✓ A short note on where risky investigative work happens today

Share it with your key stakeholder. Ask a simple question such as:

“If we give you faster, clearer intelligence on these specific threats, will it change how you act?”

SPACE FOR NOTES:

WEEK 2

Stop distributing raw indicators, start distributing decisions

★ GOAL:

Redesign at least one CTI product so it delivers decisions, not just data.

🕒 TIME REQUIRED:

6 to 8 hours total

👤 OWNER:

CTI lead with one analyst and one stakeholder

Action 1: Audit your current intelligence products

For this workflow, list what you currently send. Repeat for each major product.

Product Name: _____

Who receives it: _____

How often it goes out: _____

Does it regularly change a decision or action?

- ☐ Yes
- ☐ No
- ☐ Sometimes

Product Name: _____

Who receives it: _____

How often it goes out: _____

Does it regularly change a decision or action?

- ☐ Yes
- ☐ No
- ☐ Sometimes

Product Name: _____

Who receives it: _____

How often it goes out: _____

Does it regularly change a decision or action?

- ☐ Yes
- ☐ No
- ☐ Sometimes

Product Name: _____

Who receives it: _____

How often it goes out: _____

Does it regularly change a decision or action?

- ☐ Yes
- ☐ No
- ☐ Sometimes

Action 2: Pick one product to redesign

Choose your most frequent or most visible product for this workflow. For many teams, this is:

- A daily or weekly indicator list, or
- A recurring “here is what is happening” survey

Product we are redesigning in week 2:

Action 3: Define a decision ready template

For this workflow, decision ready intelligence must be short and actionable. Use a template like this:

- **Threat:** What is happening
- **Relevance:** Why this matters for us, based on Week 1 mapping
- **Exposure:** Where we are affected, if known
- **Recommendation:** What we should do
- **Timeline:** When we should act
- **Assumptions and gaps:** What we do not know yet

Turn this into a one page template your team can fill in quickly.

Action 4: Decide where high risk analysis will happen

Before using the new template, decide where any risky analysis will run:

- Opening suspicious documents related to this threat
- Visiting adversary infrastructure
- Testing detection content, rules, or blocking policies

Set a simple rule for this workflow:

For this workflow, analysts handle high risk content in:

- Our secure analyst environment or sandbox
- A defined, isolated lab network

and never in:

- Standard user workstations
- Ad hoc, unmanaged virtual machines

Write this rule into your internal runbook.

Establish SLAs for decision-speed

Agree with stakeholders on how fast CTI needs to respond for this workflow, and start measuring it.

4 to 6 hours total

CTI lead with
key stakeholders

Meet with:

- ✓ The operational owner (SOC, vulnerability, fraud, etc.)
- ✓ The business or risk owner, if there is one

Ask questions like:

- When a new threat or vulnerability touches this workflow, how soon do you need to know if we are affected
- What are recent examples where CTI was too slow
- If we could consistently meet a certain response time, what would that change for you

Capture answers in simple notes.

SPACE FOR NOTES:

Action 2: Draft a simple SLA matrix

Define three priority tiers for this workflow and timelines that are realistic.

Example only, adjust for your reality:

Critical:

- **Definition:** Active exploitation that could hit the crown jewels for this workflow
- **Relevance assessment:** within 2 to 4 hours
- **Decision ready brief:** within 8 hours

High:

- **Definition:** Emerging campaigns, clear sector targeting, or high impact vulnerabilities
- **Relevance assessment:** within 24 hours
- **Decision ready brief:** within 48 hours

Medium:

- **Definition:** Strategic trends or lower urgency issues
- **Summary and recommendations:** within 3 to 5 days

Write your own definitions and times in a small table.

PRIORITY	DEFINITION	RELEVANT ASSESSMENT	DECISION READY BRIEF
CRITICAL			
HIGH			
MEDIUM			
LOW			

Action 3: Include environment readiness in your plan

Be explicit about the role of secure environments in meeting these SLAs. For example:

- For Critical and High, analysts will use pre approved secure analysis environments so they do not lose time building one off labs or requesting exceptions.

If environment access is currently slow or manual, note that as a risk and an improvement target.

Action 4: Review and agree

Share the draft SLA matrix with stakeholders:

- ✓ Confirm that the definitions make sense
- ✓ Confirm that the timelines would materially help them
- ✓ Agree on how to handle true exceptions and escalations

Capture any final changes and publish the SLA internally.

Action 5: Start measuring against the SLA

For the next several events that touch this workflow:

For each event, record:

- ✓ Time of first relevant signal
- ✓ Time of first relevance assessment
- ✓ Time of first decision ready brief

Compare these times to your SLA targets. You are not aiming for perfection in week 3. You are creating a baseline.

Week 3 Deliverable

A one page SLA document for this workflow that includes:

- ✓ Priority tiers and definitions
- ✓ Target timelines for relevance assessments and decision ready briefs
- ✓ A note on which secure environments analysts will use for high risk analysis
- ✓ A simple log of recent events and your actual times

WEEK 4

Automate one high volume, low value task

★ GOAL:

Free analyst time for higher value work by automating something repetitive in this workflow.

🕒 TIME REQUIRED:

8 to 12 hours, depending on tooling

👤 OWNER:

CTI lead or senior analyst with a platform owner

Action 1: Identify your top time sinks

Ask your analysts for this workflow:

- ✓ Which tasks feel repetitive and mechanical
- ✓ Which tasks they would gladly hand off to a script or automation

Common candidates:

- ➔ Normalizing and deduplicating feed data
- ➔ Basic indicator enrichment (whois, reputation, geolocation)
- ➔ Tagging items with standard labels or priority
- ➔ Manually provisioning and tearing down analysis environments

List the top 3:

1. _____
2. _____
3. _____

Action 2: Pick one task to automate

Choose a task that:

- ✓ Happens often
- ✓ Has a clear input and output
- ✓ Does not require human judgment

Task to automate in week 4:

Action 3: Check what your current tools can do

Look at:

- ✓ Threat intelligence platform automation features
- ✓ SIEM and SOAR workflows
- ✓ Existing internal scripts or playbooks
- ✓ Options to standardize secure environment provisioning for this task

RULE FOR THIS WEEK:

Use existing tools first. Do not design a new platform.

Action 4: Design and implement a simple workflow

Describe the automation step by step.

For example, for data processing:

1. Ingest new data from source X
2. Run enrichment A, B, C
3. Remove duplicates and low confidence items
4. Tag remaining items with standard labels
5. Store in system Y and notify analyst in channel Z

For environment related tasks, it might be:

1. Analyst requests an analysis environment for this workflow
2. System creates a pre configured sandbox with required tools and logging
3. Analyst receives access details within a few minutes
4. Environment is cleaned up automatically after use

Work with platform or engineering contacts to implement and test.

SPACE FOR NOTES:

Action 5: Measure time saved and decide how to use it

Before and after automation, estimate:

- ✓ Time per run of the task
- ✓ How many times per week it runs

Rough calculation is enough. For example:

- **Before:** about 45 minutes, 4 times per week
- **After:** about 10 minutes, 4 times per week
- **Time saved:** about 2 hours and 20 minutes per week

Agree as a team how to use that time. Examples:

- More proactive analysis for this workflow
- Better stakeholder updates
- Designing the next improvement to decision-speed

Week 4 Deliverable

One automated workflow that reduces manual work in your chosen CTI workflow and:

- ✓ Is documented
- ✓ Is known to analysts
- ✓ Has an approximate estimate of time saved

SPACE FOR NOTES:

BEYOND 30 DAYS

Build momentum

These four weeks will not transform your CTI program on their own, but they will create visible improvements you can point to:

- ✓ A clearer mapping between threats and business context for at least one workflow
 - ✓ At least one decision ready CTI product that stakeholders recognize and use
 - ✓ Shared expectations for response times in that workflow
 - ✓ Less manual work for analysts on one recurring task
-

From here you can:

- ✓ Apply the same pattern to a second workflow, such as vendor risk or incident postmortems
 - ✓ Expand automation and contextualization so your team can support more decisions without adding headcount
 - ✓ Extend CTI support beyond security to product, legal, regional expansion, and other business teams
 - ✓ Standardize secure analysis environments and sandboxes across more types of high risk work, so analysts never have to improvise on production systems
-

At the end of each 30 day cycle, run a short review:

1. What changed that matters to stakeholders
2. What sped up and by how much
3. Which secure environment or automation changes had the most impact
4. What you want to improve in the next cycle

The goal is progress, not perfection. Every small increase in decision-speed and relevance builds trust. Over time, that trust is what turns CTI from a data function into an asset that shapes how the organization moves.