An aerial photograph of a city, likely Copenhagen, featuring a river, a bridge, and a prominent tall tower (Copenhagen Tower). The image is overlaid with a semi-transparent dark grey filter.

How to Start Using Priority Intelligence Requirements (PIRs) on a Budget

Josh Darby MacLellan

Josh@feedly.com


Core problem uniting CTI

Mounting pressure
to do more with
less time, budget,
and headcount



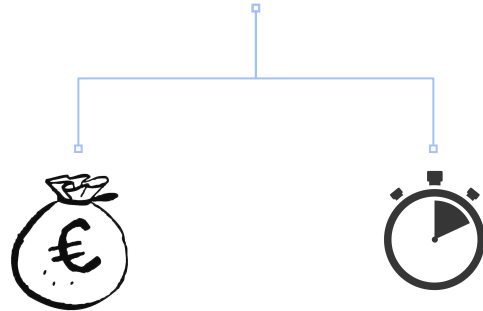
The solution:

prioritized topics that
stakeholders need intelligence
on to make better decisions

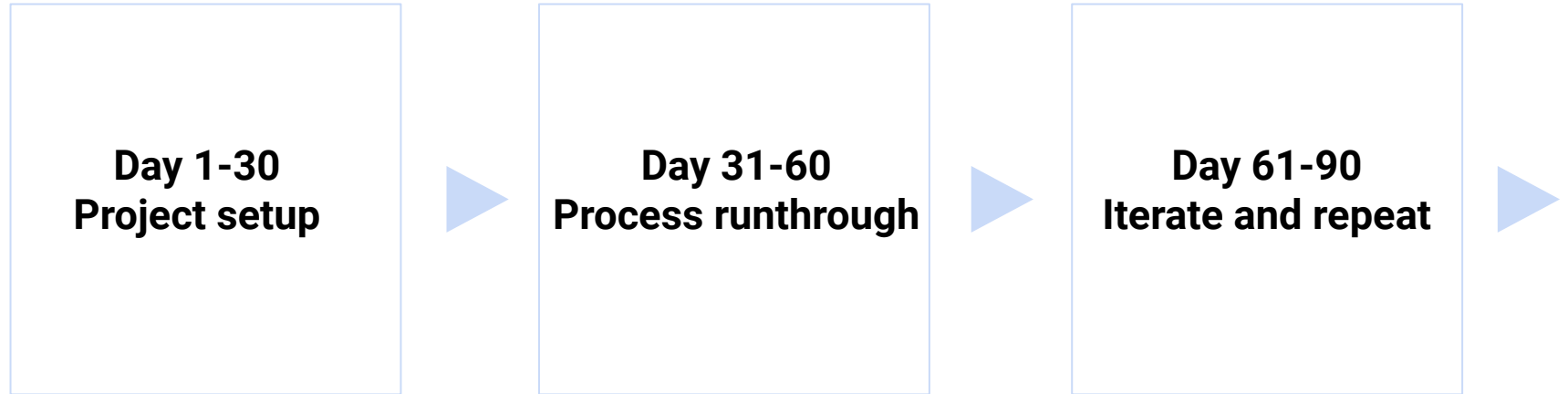


That'll be €10k

How to Start Using Priority Intelligence Requirements (PIRs) on a Budget




Overview



Day 1-30

Project setup

A photograph of two business women sitting at a wooden table in a modern office setting. The woman on the left is wearing a light blue blazer and has her hands clasped. The woman on the right is wearing a light-colored blazer and is looking at a laptop. The background shows a bright office with large windows and a bookshelf.

**Why take the stakeholder
interview approach?**

Stakeholder interview benefits

- 1 Tap into experience
- 2 Relationship-building mechanism
- 3 We don't know what we don't know

A system to track time investment



MON

20

TUE

21

WED

22

THU

23

FRI

24

JANUARY 20 - 24

Time Insights



Zürich design days

Pick up new bike

Time breakdown ?



By type

By color



- Important 2 hr
 - Personal 5 hr
 - Strategy 2022 3 hr
 - Other 15 hr
 - Remaining 4.5 hr
- Based on your working hours

Adjust working hours

Win leadership's approval

The Case for Implementing Priority Intelligence Requirements

Priority Intelligence Requirements (PIRs) a set of mission critical topics that stakeholders need intelligence on to inform their decision-making. Here are some of the key benefits:

Benefits for the CTI Team

- Provides clear direction and focus [\[1\]](#)
- Allows efficient allocation of limited resources [\[2\]](#)
- Enables effective prioritization [\[3\]](#)
- Provides metrics to demonstrate value [\[4\]](#)

Benefits for Stakeholders

- Aligns intelligence collection to their needs [\[5\]](#)
- Provides visibility into relevant threats [\[6\]](#)
- Enables stakeholder participation [\[7\]](#)

Benefits for the Business

- Focuses limited resources on critical threats [\[8\]](#)
- Provides intelligence tailored to the organization [\[9\]](#)
- Demonstrates return on investment [\[8\]](#)

In summary, PIRs enable CTI teams to provide maximum value to stakeholders while efficiently allocating limited resources. This ultimately translates to better security outcomes and demonstrated ROI for the business. I would be happy to discuss this further and address any additional questions or concerns.



The Case for Implementing Priority Intelligence Requirements

Priority Intelligence Requirements (PIRs) are a set of mission critical topics that stakeholders need intelligence on to inform their decision-making. Here are some of the key benefits:

Benefits for the CTI Team

- Provides clear direction and focus [\[1\]](#)
- Allows efficient allocation of limited resources [\[2\]](#)
- Enables effective prioritization [\[3\]](#)
- Provides metrics to demonstrate value [\[4\]](#)

Benefits for Stakeholders

- Aligns intelligence collection to their needs [\[5\]](#)
- Provides visibility into relevant threats [\[6\]](#)
- Enables stakeholder participation [\[7\]](#)

Benefits for the Business

- Focuses limited resources on critical threats [\[8\]](#)
- Provides intelligence tailored to the organization [\[9\]](#)
- Demonstrates return on investment [\[8\]](#)

In summary, PIRs enable CTI teams to provide maximum value to stakeholders while efficiently allocating limited resources. This ultimately translates to better security outcomes and demonstrated ROI for the business. I would be happy to discuss this further and address any additional questions or concerns.

Research your organization

“If you understand your business,
you’ll understand your stakeholders”

- A famous person






How does your
organization make money?

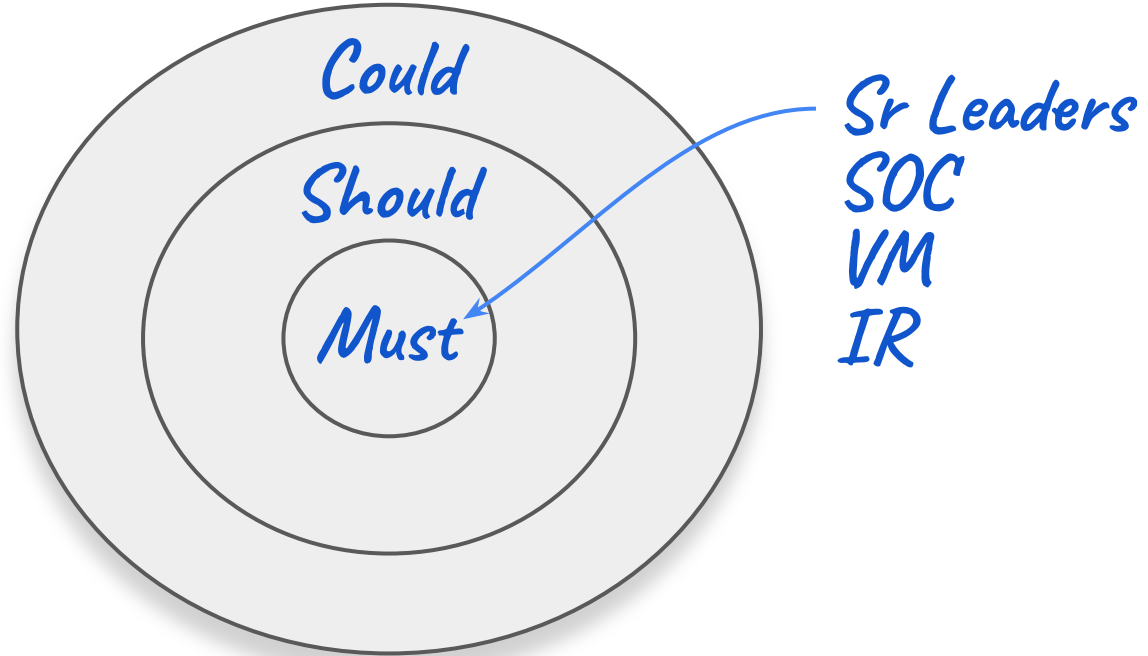
A close-up photograph of a person's face, with their eyes looking directly at the camera. They are holding a large fan of US dollar bills in front of their mouth and nose. The bills are fanned out, showing various denominations including \$100, \$20, and \$10. The text "Who makes that money and where?" is overlaid in white, bold, sans-serif font across the center of the image.

**Who makes that money
and where?**



**What do they need to
make that money?**

Map your stakeholders



**Map PIR process in prep
for first run through**



Your team

Your fav
stakeholder



Day 31-60

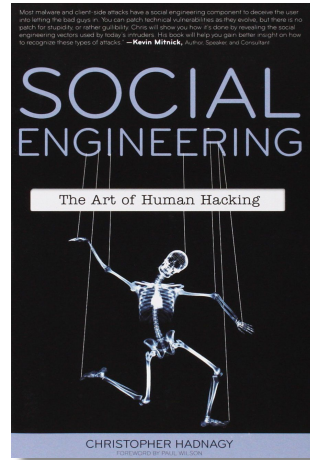
Process runthrough

Book first stakeholder interview

Stakeholder Interview Scheduling Email template

Download the example email as a word doc.

[CLICK TO DOWNLOAD](#)



Do (a lot of) interview prep

The Six Ps

Perfect

Planning

Prevents

Piss

Poor

Performance

Tailor questions

1

What is your top concern related to cyber threats that could affect your team's operations?

2

What are the most critical assets that your team needs to have protected?

3

How would you ideally like to receive intelligence?

E.g. via email, Slack/Teams, briefings, video call, etc.

Additional example questions

TLP:AMBER



Section 2: Intelligence support

Record the use-cases requiring intelligence support and deliverables. Ask your stakeholder the following questions:

4. Generally, what intelligence information do you need to do your job? What keeps you up at night?

5. What is your success criteria? How will you be satisfied with the intelligence support we provide you?

6. What use cases do you need intelligence support for?

check all that apply

- Network and endpoint protection
- Penetration testing and attack emulation
- Vulnerability and patch management
- Insider threat
- Threat hunting
- Risk and compliance
- Fraud
- Identity management
- Other:

7. What type of product/service do you prefer for intelligence support?

check all that apply

- Formal Report
- Regular Briefing
- IOC feed data
- On demand requests for information (RFI)
- Other:

8. How do you prefer to submit requests for information (RFI) to us?



Tip during the interview

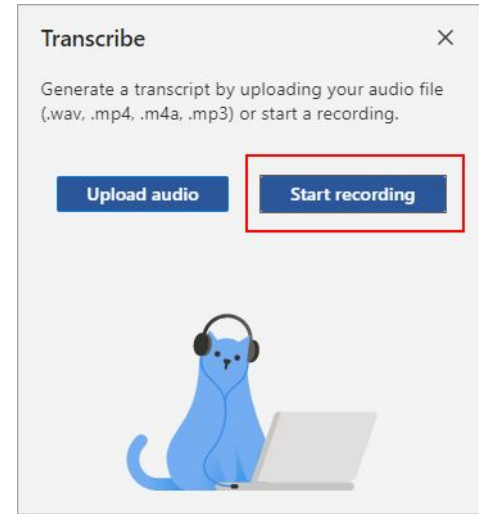
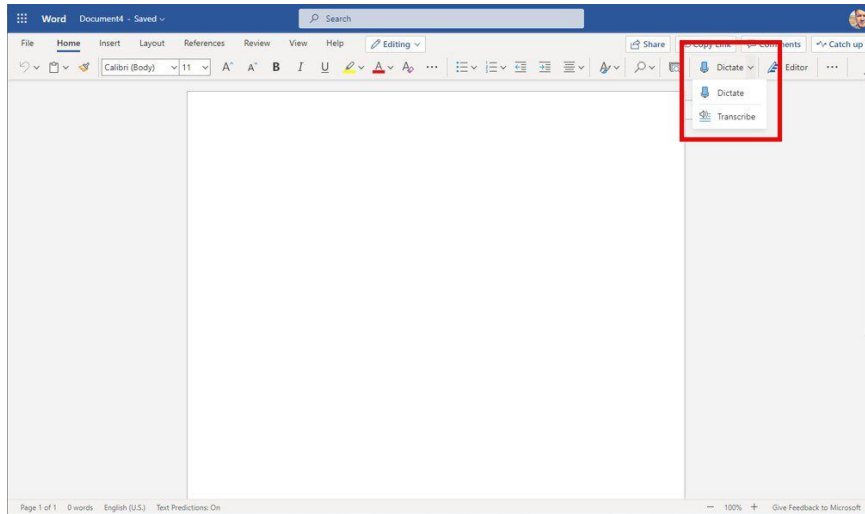
Go hands free

Talk about the weather

Don't steal time

Show gratitude post-interview

How to go hands free



Chats

+ New Chat (⌘N)

Export

Reload to apply configuration

Plaintext Markdown

Settings

Reset to Default Settings

Untitled Chat

Quick method to process interview data

Chat with a Large Language Model

- Sending messages as USER will trigger inferencing
- Config parameters are sticky (auto-save upon changes).
- Double click on any message to edit its contents
- Click the USER button next to the chat box to toggle between USER and ASSISTANT roles
- Sending messages as ASSISTANT will not trigger inferencing

Reload model to apply configuration

USER

Reload the model to continue

0 tokens

↵ to send, shift + ↵ for new line

Below is an instruction that describes a task. Write a response that appropriately completes the request.

Ask before overriding

GPU Acceleration

Show Help

Apple Metal (GPU) n_gpu_layers 10



Quick GPU Offload Settings

Low 50/50 Max

Tools

Model Inspector

Context Overflow Policy

Behavior for when the generated tokens length exceeds the context window size.

- Stop at limit
- Keep the system prompt and the first user message, truncate middle
- Maintain a rolling window and truncate past messages (default)

Conversation Notes

What makes a good PIR question?

Singular question

Intel answerable

Specific

Time-sensitive

Support decisions



Document PIRs in simple spreadsheet

Priority level

Collection plan

Intel deliverable

# PIR	Priority (1-10)	Stakeholders	Collection plan				Deliverable(s)		
			Threat intel feed	CTI Vendor	OSINT	Darkweb Scrapper	Ad-Hoc Threat Intel Brief	Instant Message	Monthly Intel Report
1	10	SOC, IR, VM, MGM	x		x	x	x	x	
2	9	SOC, VM, IR	x	x	x			x	
3	8	TH, MGM		x	x		x		x
4	8	SOC, TH, VM	x			x	x		x
5	6	SOC, MGM		x	x	x			x
6	6	SOC, IR, VM, MGM	x		x	x	x	x	

Stakeholders

A futuristic control room with multiple large screens displaying data and a person in a hoodie pointing at a central screen. The room is dimly lit with blue light from the screens. The central screen shows a person in a hoodie pointing at a large circular diagram. The text "CYBER THREAT INTELLIGENCE" and "ANALYSTS THEIR STRATEGIES" is visible on the screen. Other screens show various data visualizations, including a world map and various icons.

**Share PIRs and intel
deliverable prototypes**

Day 61-90

Iterate and repeat

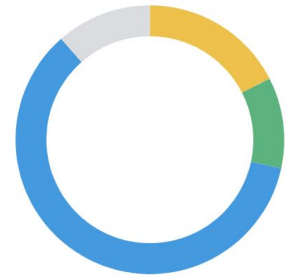
Self-reflect, analyze cost, and improve process





- What did you do well, ok, and badly?
- What took up most time?
- How many stakeholders do you have the capacity to collect PIRs from?
- How can we track ROI?

Time breakdown 

By type

By color



	Yellow	8 hr
	Green	5 hr
	Default	27.5 hr
	Remaining time	5.3 hr

Based on your working hours

[Adjust working hours](#)

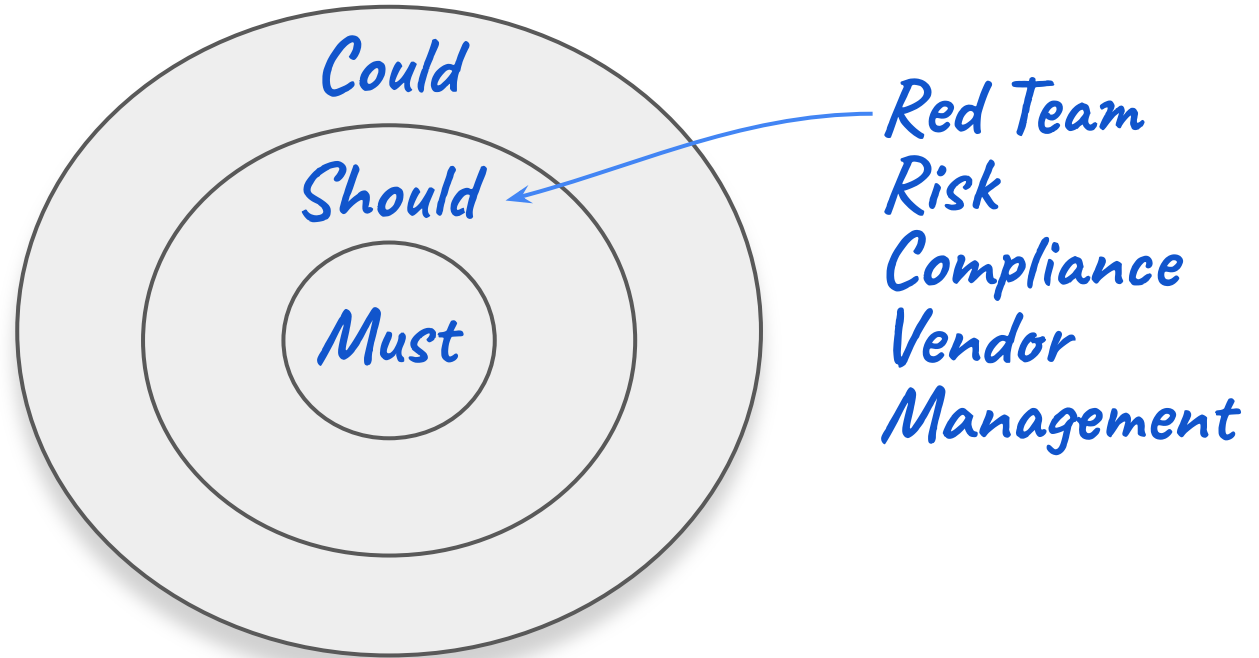
Gather and action feedback
improve process again





Run through process with VIP stakeholder

Then expand...



Recap on Day 1-90

Day 1-30: Project setup

1. Set up system to track time
2. Present business case to leadership for approval
3. Research organization, threats, and stakeholders
4. Document process in prep for first runthrough

Day 31-60: Process runthrough

5. Book first stakeholder interview
6. Do a lot of interview prep
7. Tailor questions
8. Go hands free during the interview
9. Process the interview data with LLMs
10. Document PIRs in simple spreadsheet
11. Share the PIRs and intel deliverable prototypes

Day 61-90: Iterate and repeat

12. Self-reflect, analyze cost, and improve process
13. Gather and action feedback, improve process again
14. Run through process with VIP stakeholder
15. Expand PIR collection to more stakeholders

Questions?



Josh Darby MacLellan

Josh@feedly.com

www.linkedin.com/in/josh-darby-maclellan/