If you want intelligence requirements, you do not start with intelligence requirements

(hint: you start with the actions...)

Brian Mohr
November 7, 2023
Introduction

- CEO & Cofounder – Reqfast, Inc.
- Former US Marine
- Intel Geek
- Requirements evangelist
- Husband & Father
- Furbabies owner

Brian Mohr
The state of CTI requirements today

Progress is being made!

But not enough....

Understand your role

The intelligence cycle

Actionable intelligence

Conclusion
Adoption (and acceptance) is growing
Still misunderstood
Intentions are good
We have work to do...
Common “Requirements”

- Malware
- DDoS
- Hacktivism
- Cyber Espionage
- Nation State Actors
The CTI Team sits down with the stakeholder to elicit intelligence requirements.

Should be simple, right?
“Hi there, Stakeholder! I’m Brian from the CTI team. We are a TOP-TIER intelligence team with all sorts of tools and capabilities. As INTELLIGENCE PROFESSIONALS, we know it is CRITICAL to get your INTELLIGENCE REQUIREMENTS.

So, with that being said, what are your INTELLIGENCE REQUIREMENTS?”

Um. Well… You’re the INTELLIGENCE PROFESSIONAL, aren’t you supposed to know?
The Conversation

Well, yes, but we have a lot of information, what specifically do you want to know?

Um… I guess, just tell me about the threats.

The … The threats? … Um…. Which threats?

All of them.
You want us to give you information on ‘all of the threats?’

Yes, that’s my requirement. I need to know about all of the threats.
Great. We’ll get right on that. Allllll the threats……
Open Source Release of Intel 471 Intelligence Requirements Framework

AUG 07, 2023
You Are Not Special

https://jamesbond.fandom.com/wiki/James_Bond_(Daniel_Craig)

https://www.ndtv.com/entertainment/matt-damon-i-was-grumpy-on-elysium-set-613325

You Are Not Special

I conduct cyber intelligence operations targeting threat actors in the cyber criminal underground utilizing the deep and dark web....

https://www.dailymotion.com/video/x6xryl8
Everybody “does” intel

- The Board
- The C-Suite
- The CISO
- SOC leadership
- Cyber analyst

All Decision Makers

“do intel” every day.
Intelligence is two things:

1. Decision Support
2. Customer Service
Know your role
The Intelligence Cycle

Dissemination & Feedback
Deliver your intelligence information in the format or medium the customer desires. Ensure you establish a feedback loop to identify areas of improvement.

Planning & Direction
Establish Customer Requirements / Determine what information your decision-makers need and how you plan to obtain it. Establish your stakeholder's success criteria.

Analysis & Production
Analyse your data. Try to base your assessments only on known facts and what will directly support action from leadership.

Collection & Processing
Gather the data from all your sources - both internal & external. Keep track of what you get from where.
More Cycles!

- The OODA Loop
- Agile SDL
- Project Management Lifecycle
- Risk Management Cycle
- Kaizen Process
- F3EAD
The Cycle in practice

My stakeholder is trying accomplish “A.”

They need to know “B” so they can choose between actions “X, Y, or Z.”

Did we give the right/enough “B”? 
The Cycle in practice

1. Understand stakeholder actions
2. Identify/refine information requirements
3. Collect/deliver necessary information

- Stakeholder satisfied?
  - Yes
  - No

- Incorporate Feedback

Copyright © 2023 Reqfast, Inc. All rights reserved.
To provide actionable intelligence, you have to focus on the intended actions of your stakeholder.
Actionable Intelligence

The actions of the Business:

- Increase productivity
- Reduce spending
- Maximize efficiency
- Enhance profitability
Actionable Intelligence

The actions of the CISO:

- Sustain operations
- Reduce spending
- Maximize efficiency
The CISO wants to know:

✓ Do we have what we need TODAY?

✓ Do we have what we will need TOMORROW?

✓ Can we reduce risk with what we have?

✓ Are we getting what we paid for?

✓ Where can we improve? How?
Our DDoS Protection

- How do we sustain operations?
- Do we:
  - Upgrade?
  - Replace?
  - Do nothing?

Remember: Intelligence is decision support, helping the stakeholder to choose a course of action. What do they need to know to make that choice?
Our DDoS Protection

✔ Does our DDoS tool work?
✔ Does it have limitations?
✔ Do we have too much protection? (Cyber fluff?)
✔ Does it protect against the current threat?
✔ Will it protect against the emerging threat?
✔ If not today, can it ever?
✔ What else do we have available, what else can we do?
“Hey, Bob - how are the kids? Look, I know the CISO wants us all to avoid buying new tools and making sure we make the use of what we have. But with Rapid Reset in the news, and the C-Suite and the board breathing down the CISO’s necks, I’m sure they’re coming to you.

I know you’ve been tasked with recommending whether or not we need to upgrade, buy new, or just stay the course. We have a lot of vendor connections, what outside information or information from other teams can we help you with your recommendations. What can we help you with?”
Your final pieces

- Your stakeholder’s intended actions
- Measures of success
Okay fine...

You are special

&

You are not alone
Conclusions

- Intelligence is:
  - Decision Support
  - Customer Service

- Requirements are critical, BUT

- Start with your stakeholder’s intended actions