VANITY METRICS

The Black Sheep of Cyber Security

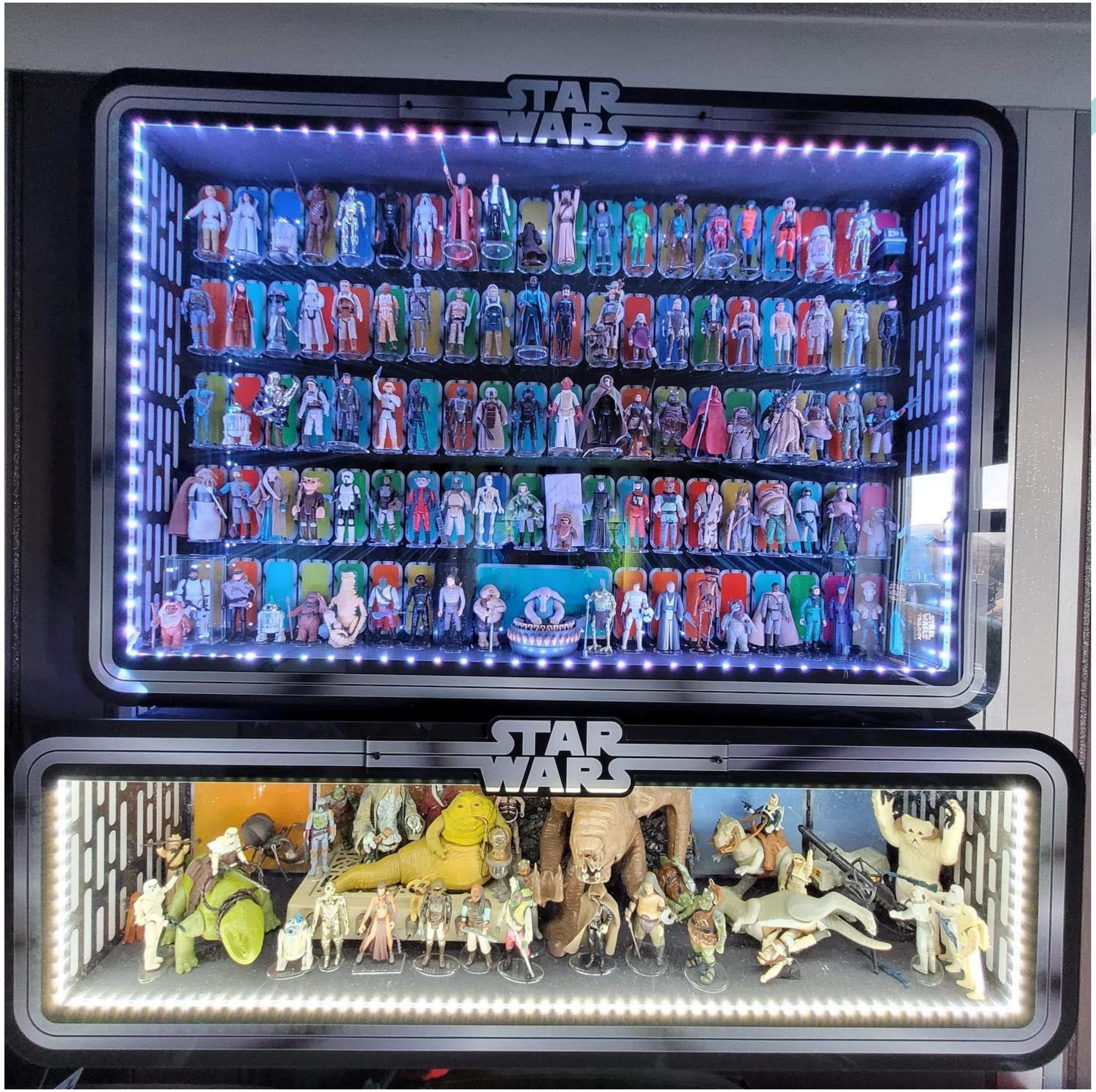
IMAGE: Tromsø, Norway (Locationscout.net)

WhoAmI

– That's All I'll Ever Be

- Freddy M
- Senior Threat Intelligence analyst @ NFCERT
- Intelligence in Army

Fun fact: I play with dolls



Agenda

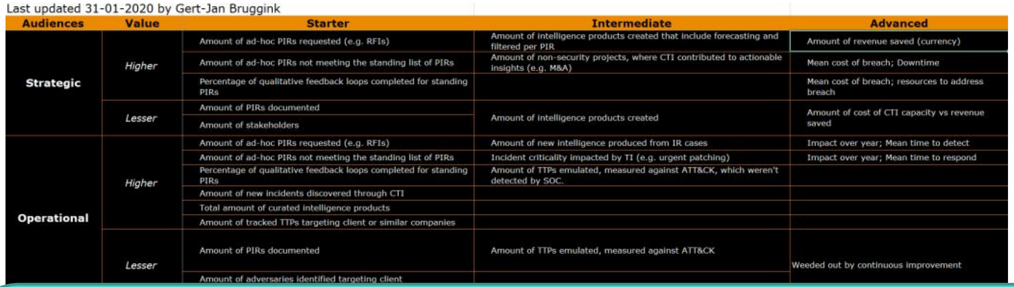
– We all have one

- Definitions, because words matter
- The Problem: Vanity Metrics
- The solution: Using the intelligence cycle to provide value through metrics

Those who came before me

– Standing on shoulders of giants

- Gert Jan Bruggink - METRIC
- https://github.com/gertjanbruggink/Metrics



Last updated 31-01-2020 by Gert-Jan Bruggink

Audiences	Value	Starter	Intermediate	Advanced
Strategic	Higher	Amount of ad-hoc PIRs requested (e.g. RFIs)	Amount of intelligence products created that include forecasting and filtered per PIR	Amount of revenue saved (currency)
		Amount of ad-hoc PIRs not meeting the standing list of PIRs	Amount of non-security projects, where CTI contributed to actionable insights (e.g. M&A)	Mean cost of breach; Downtime
		Percentage of qualitative feedback loops completed for standing PIRs		Mean cost of breach; resources to address breach
	Lesser	Amount of PIRs documented	Amount of intelligence products created	Amount of cost of CTI capacity vs revenue saved
		Amount of stakeholders		
Operational	Higher	Amount of ad-hoc PIRs requested (e.g. RFIs)	Amount of new intelligence produced from IR cases	Impact over year; Mean time to detect
		Amount of ad-hoc PIRs not meeting the standing list of PIRs	Incident criticality impacted by TI (e.g. urgent patching)	Impact over year; Mean time to respond
		Percentage of qualitative feedback loops completed for standing PIRs	Amount of TTPs emulated, measured against ATT&CK, which weren't detected by SOC.	
		Amount of new incidents discovered through CTI		
		Total amount of curated intelligence products		
		Amount of tracked TTPs targeting client or similar companies		
	Lesser	Amount of PIRs documented	Amount of TTPs emulated, measured against ATT&CK	Weeded out by continuous improvement
		Amount of adversaries identified targeting client		

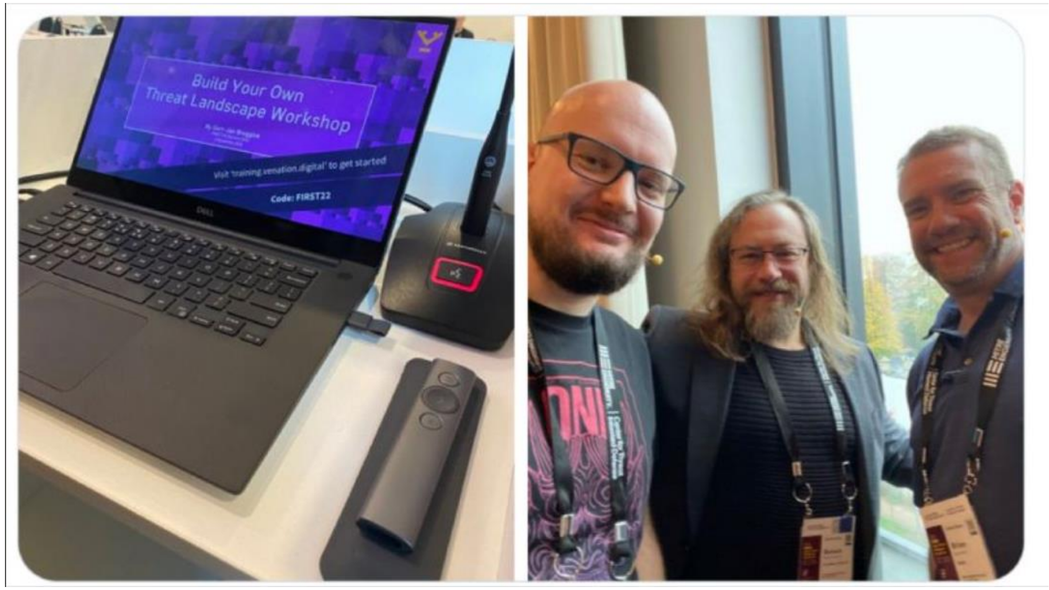
- Marika Chauvin & Toni Gidwani "How to get Promoted" @ SANS CTI Summit 2019

How to Get Promoted: Metrics to Show How

"How can we show that our Cyber Threat Intelligence program provides value to our organisation?"

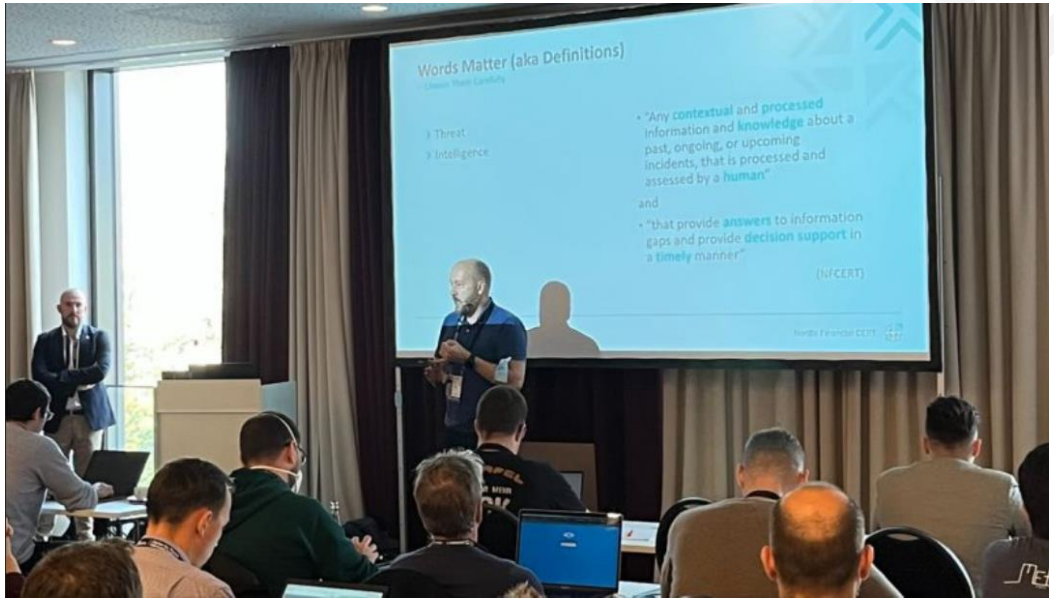
Yesterday’s Workshops

‘Build Your Own Threat Landscape’


Build Your Own
Threat Landscape Workshop
Visit 'training.venation.digital' to get started
Code: FIRST22

Gert-Jan, Roman and Brian

Intelligence Planning


Words Matter (aka Definitions)
Threat
Intelligence
• "Any contextual and processed information and knowledge about a past, ongoing, or upcoming incidents, that is processed and assessed by a human"
and
• "that provide answers to information gaps and provide decision support in a timely manner"
(NFCERT)

Joseph, Brad and Freddy

Definitions

– Words actually matter

- Metrics

Definition: Measures of quantitative or qualitative assessment commonly used for comparing, and tracking performance or production

Goal: Metrics permits a business to monitor for changes in order to take action

Value:

- Decision Support
- Reducing Uncertainty
- Situational Awareness (Increasing Awareness)

Definitions

– Words actually matter

- **Vanity Metrics**
- Stakeholder

All those pieces of data that feel great when they go up, but make no real difference to

- Success
- Decision
- Uncertainty
- Situational Awareness

They look great, but provide no real value to the stakeholder

Definitions

– Words actually matter

- Vanity Metrics
- **Stakeholder**

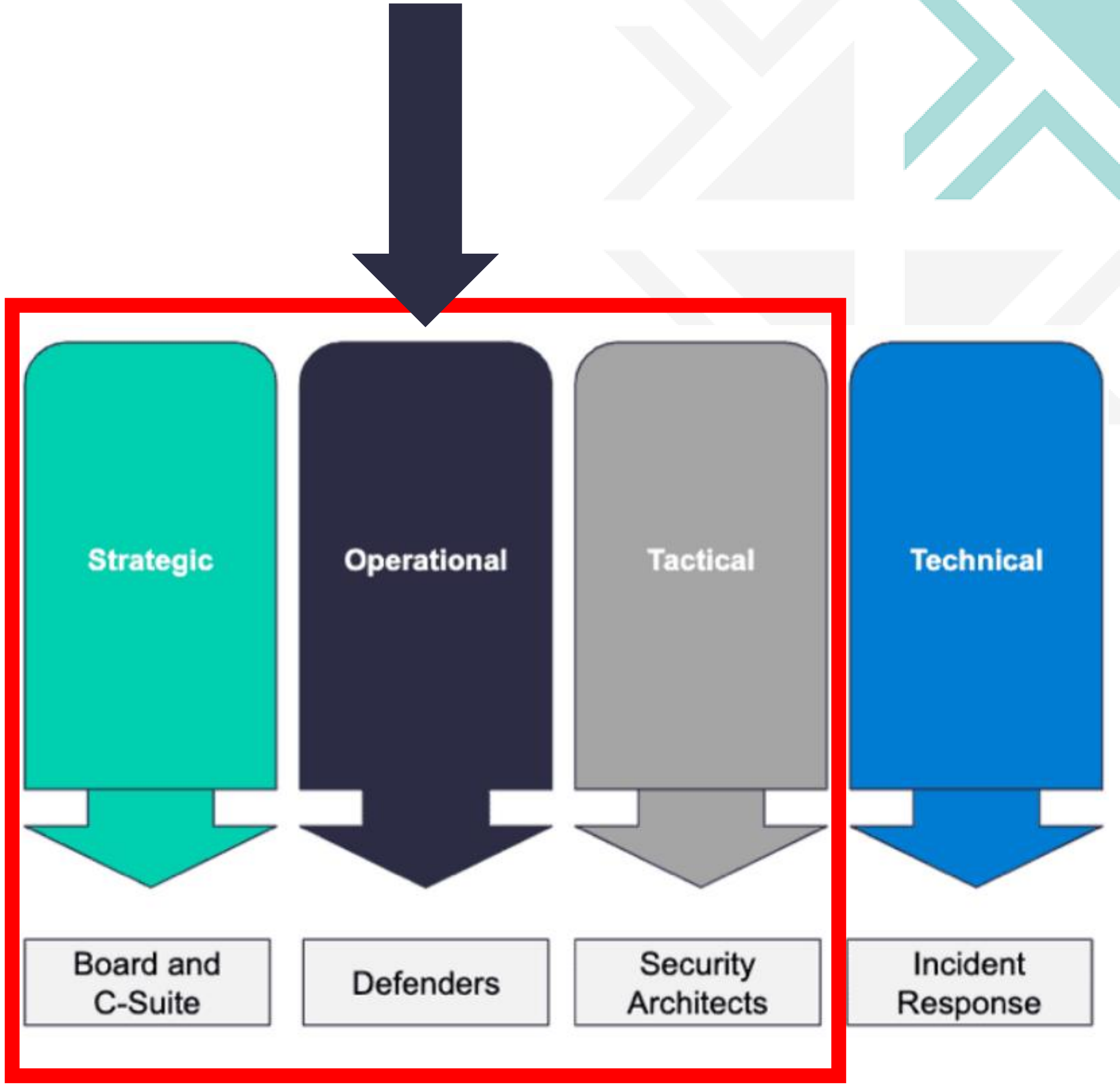
A stakeholder is anyone who has any interest/influence in what you are doing

Stakeholders will determine the **success**, or **not**, of your projects and activities

Framing the Issue

– Seeing eye to eye

- Metrics are good and serve a purpose
  - …..as long as they are used correctly and not “gamed” to show “your truth”
- In this context
  - Measuring the success of our CTI →**program**← not just the product or process
  - “Why we are here”
- Operational level, supporting both Strategic AND Tactical



Source: Digital Shadows - “Threat Intelligence: A deep Dive”

Gaming

– A Fundamental Issue

Campbell's Law

The more a metric is visible and used to make **important** decisions, the more it will be gamed…

…which will distort and corrupt the exact processes it was meant to monitor

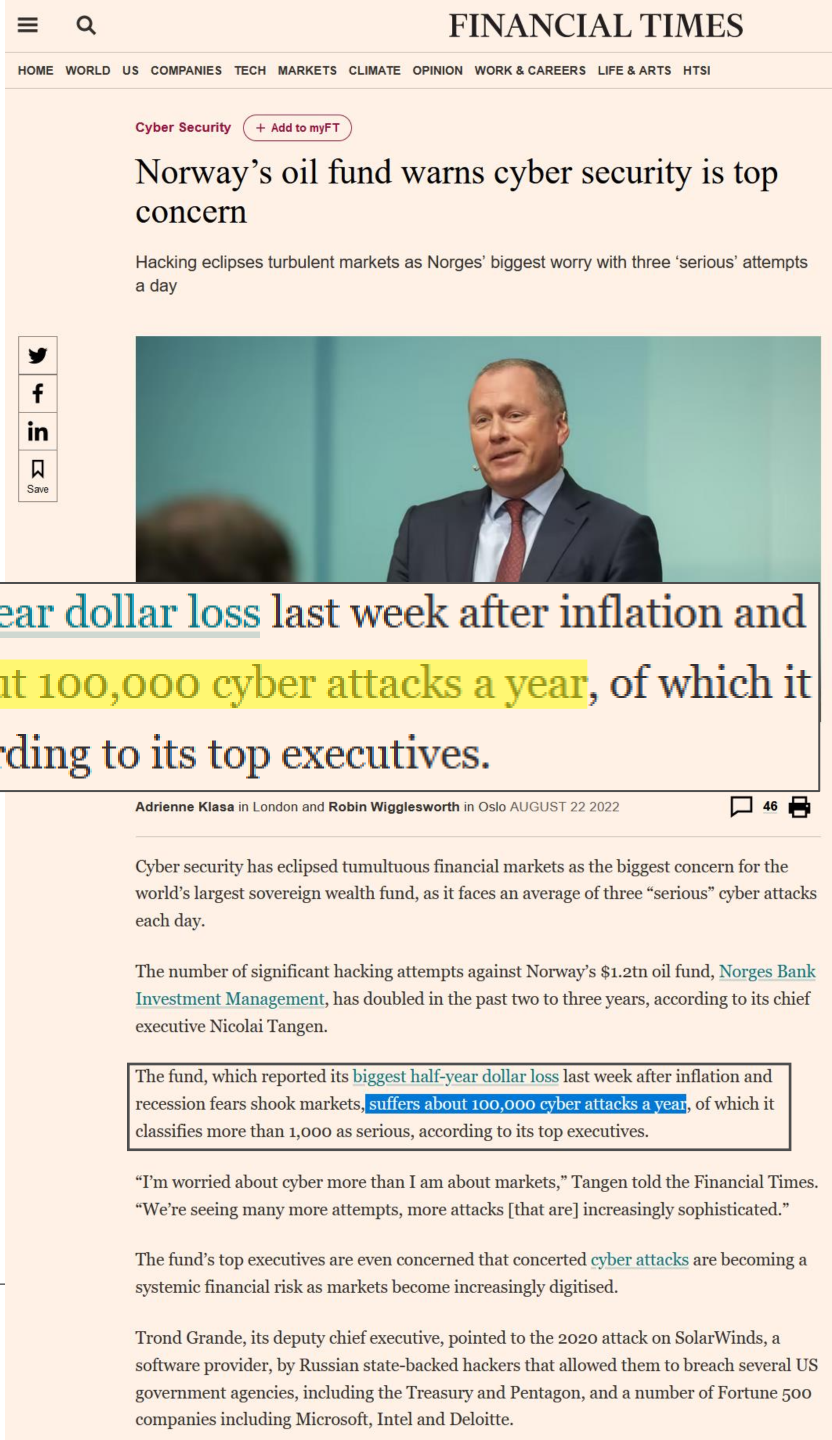
Goodhart's Law

Anything that can be measured and rewarded will be gamed

Management is shown metrics where the number of attacks have increased year over year….

- What constitutes an «attack»?
  - Port scanning?
  - Vulnerability scanning?
  - Phishing emails?
- Detections vs Alerts?
  - False positives?
  - Ratio?
- Script kiddies versus attacks from sophisticated attackers
- How many of the alerts would have resulted in a breach?
- Should focus on VALUE rather than VOLUME

The fund, which reported its biggest half-year dollar loss last week after inflation and recession fears shook markets, suffers about 100,000 cyber attacks a year, of which it classifies more than 1,000 as serious, according to its top executives.



FINANCIAL TIMES
HOME WORLD US COMPANIES TECH MARKETS CLIMATE OPINION WORK & CAREERS LIFE & ARTS HTSI
Cyber Security
+ Add to myFT
Save
46

Norway's oil fund warns cyber security is top concern

Hacking eclipses turbulent markets as Norges' biggest worry with three 'serious' attempts a day

Adrienne Klasa in London and Robin Wigglesworth in Oslo AUGUST 22 2022

Cyber security has eclipsed tumultuous financial markets as the biggest concern for the world's largest sovereign wealth fund, as it faces an average of three "serious" cyber attacks each day.

The number of significant hacking attempts against Norway's $1.2tn oil fund, Norges Bank Investment Management, has doubled in the past two to three years, according to its chief executive Nicolai Tangen.

The fund, which reported its biggest half-year dollar loss last week after inflation and recession fears shook markets, suffers about 100,000 cyber attacks a year, of which it classifies more than 1,000 as serious, according to its top executives.

"I'm worried about cyber more than I am about markets," Tangen told the Financial Times. "We're seeing many more attempts, more attacks [that are] increasingly sophisticated."

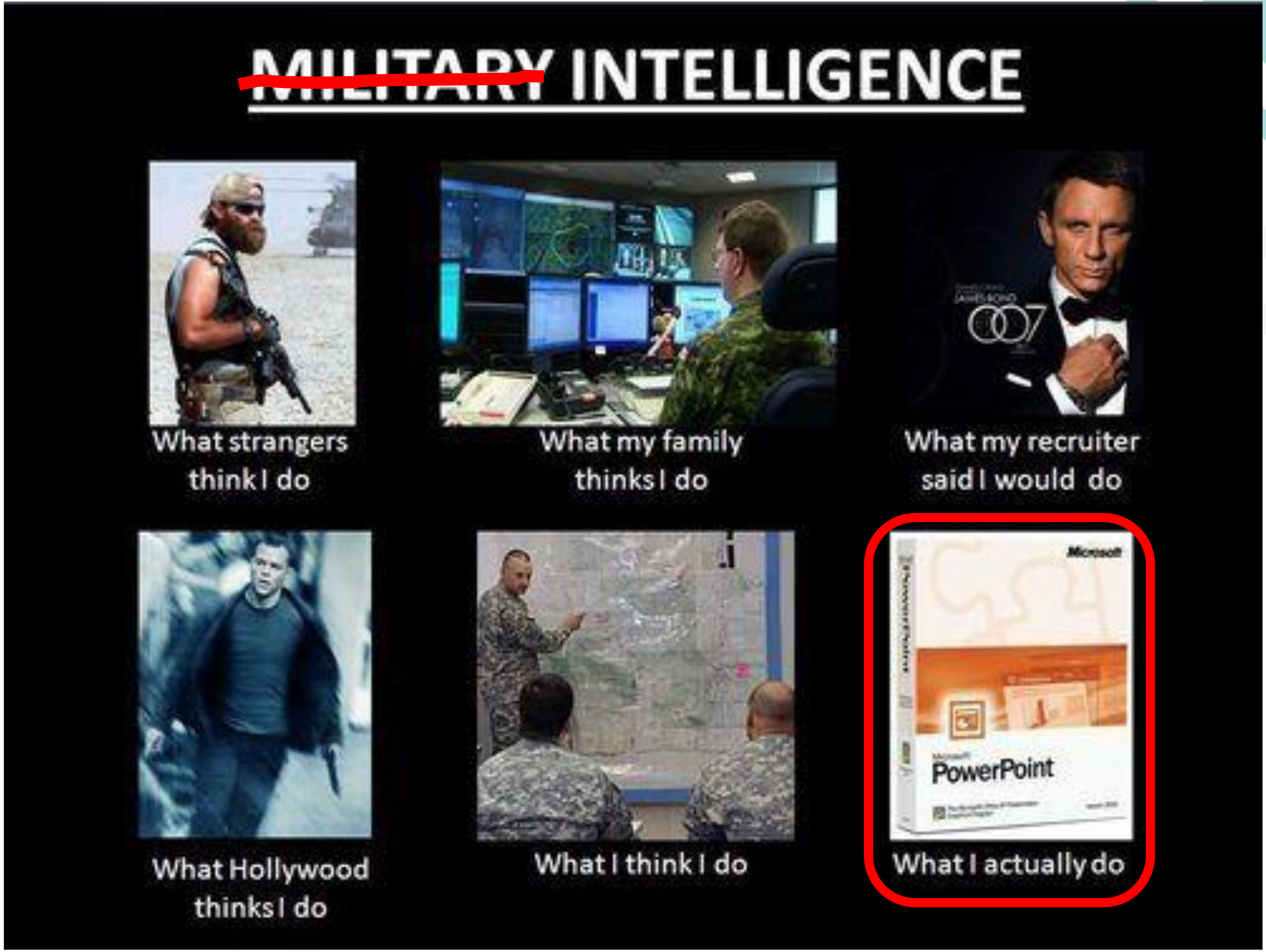
The fund's top executives are even concerned that concerted cyber attacks are becoming a systemic financial risk as markets become increasingly digitised.

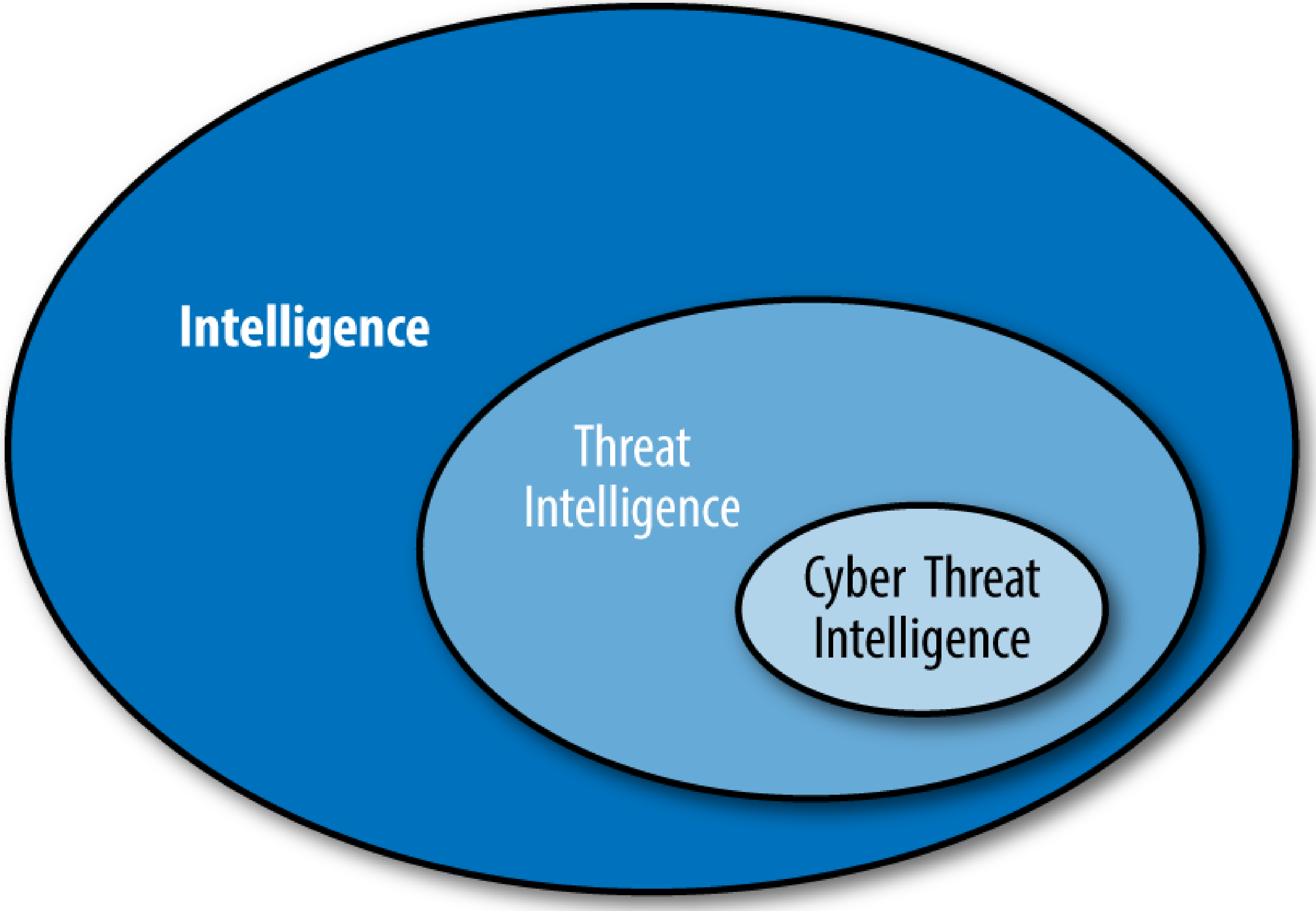
Trond Grande, its deputy chief executive, pointed to the 2020 attack on SolarWinds, a software provider, by Russian state-backed hackers that allowed them to breach several US government agencies, including the Treasury and Pentagon, and a number of Fortune 500 companies including Microsoft, Intel and Deloitte.

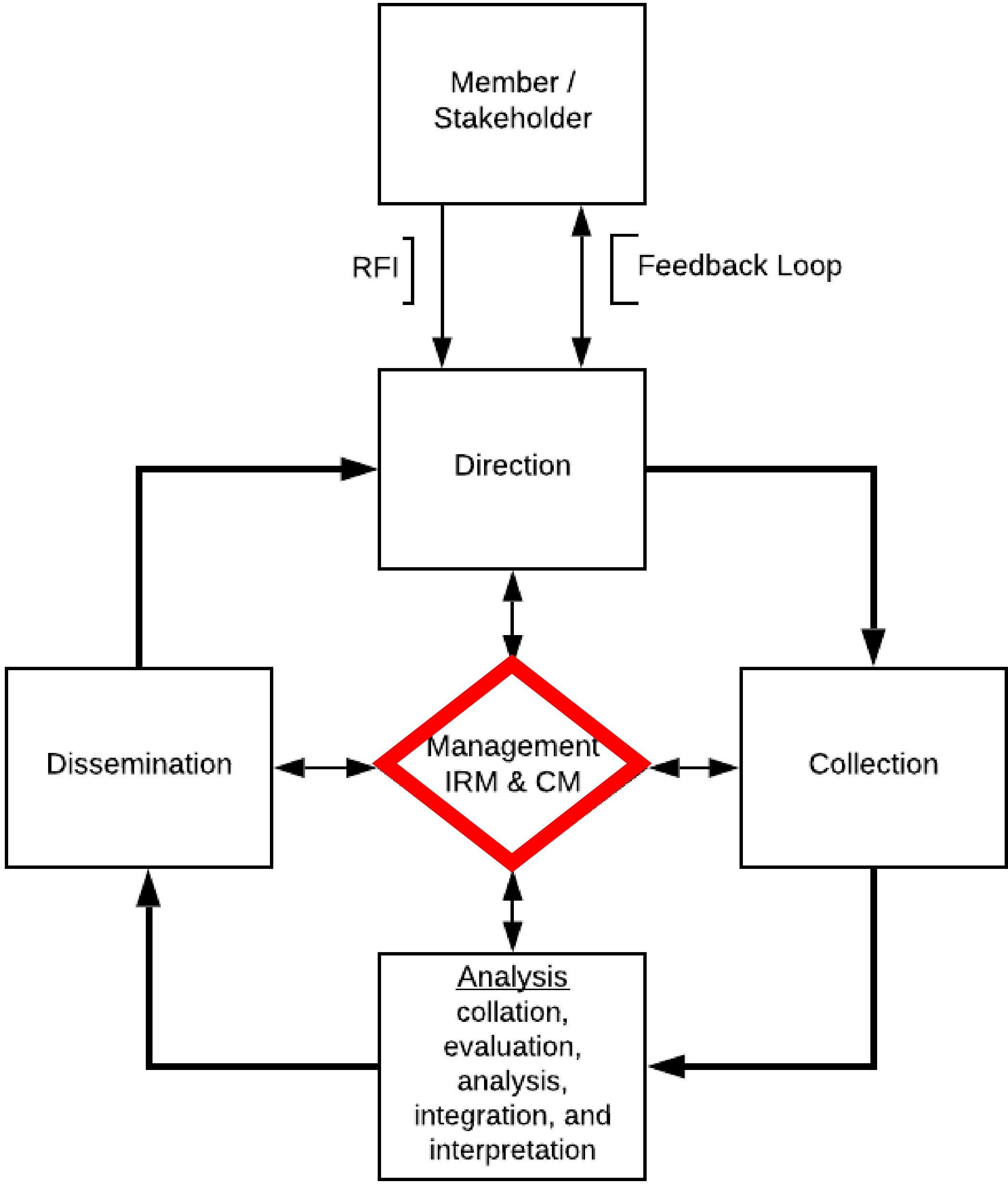
Intelligence

– Not just for the government

- Product
- Process
- Program

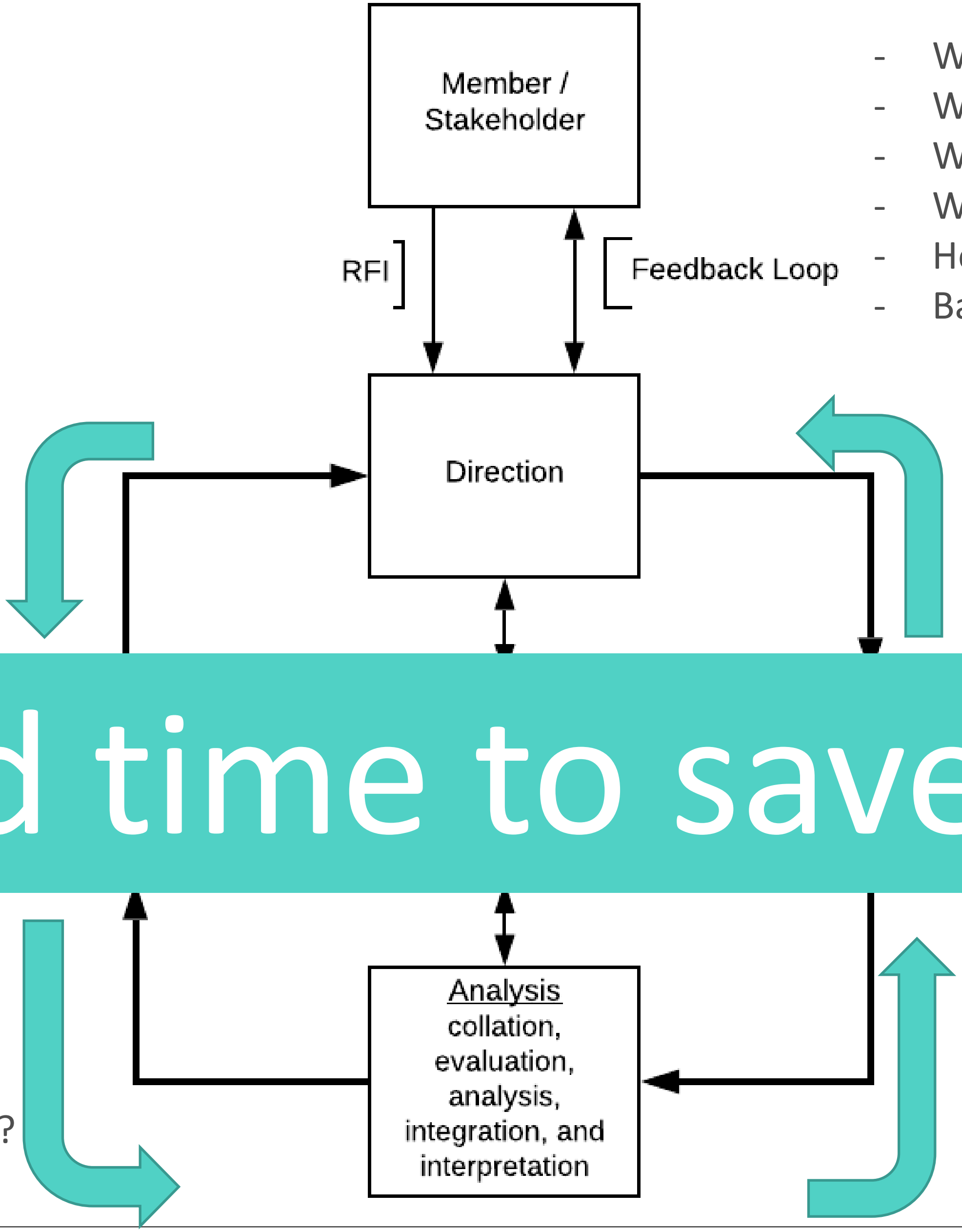

~~MILITARY~~ INTELLIGENCE
What strangers think I do
What my family thinks I do
What my recruiter said I would do
What Hollywood thinks I do
What I think I do
What I actually do
PowerPoint


Intelligence
Threat Intelligence
Cyber Threat Intelligence


Member / Stakeholder
RFI
Feedback Loop
Direction
Dissemination
Management IRM & CM
Collection
Analysis
collation, evaluation, analysis, integration, and interpretation

Spend time to save time

- Who is the consumer/stakeholder?
- What does she want to know?
- Why does she want it?
- When does she want it?
- What type of product does she want?
- How does she want it delivered?


Member / Stakeholder
RFI
Feedback Loop
Direction
Analysis
collation, evaluation, analysis, integration, and interpretation

- What she wants to know, rephrased
- What function/process we are supporting
- When she wants it
- What type of product she wants
- How I will work through the steps
- Based on feedback, make adjustments

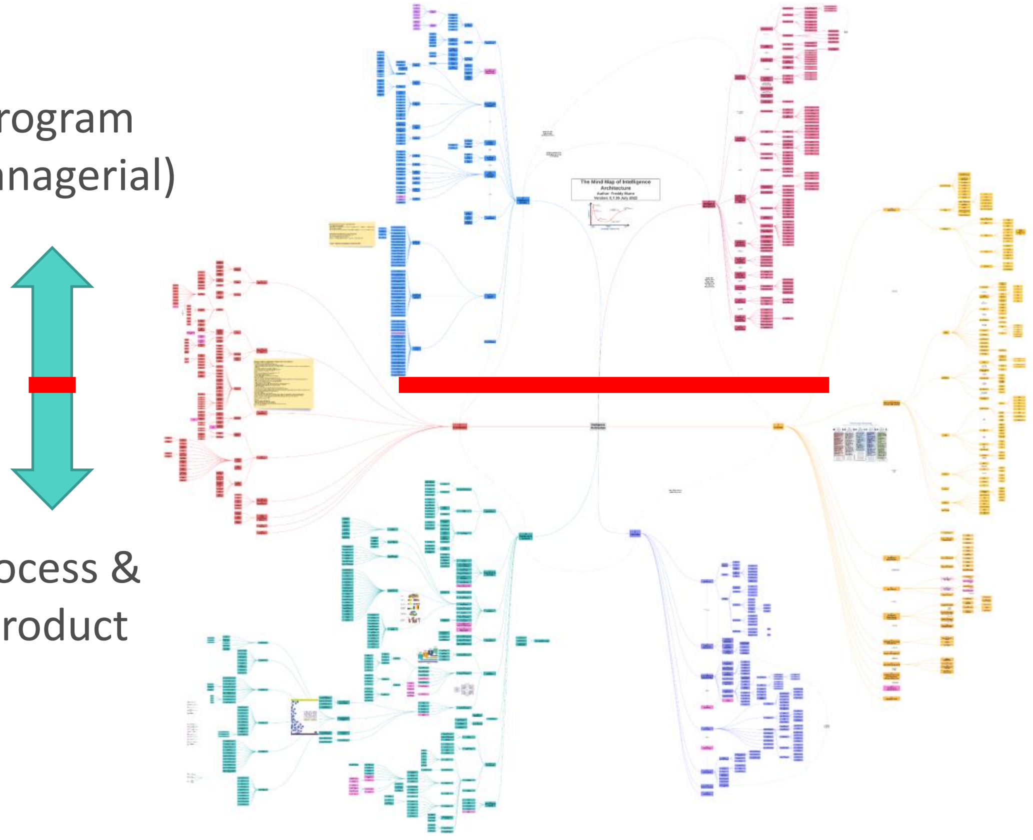
nce

What do we know/not know?
  - Discover Intel gaps
- Where to collect from?
  - Do we have access?
  - Do we have to develop access?
- Who will collect it?
- How long will it take?

- What type of analysis are we doing?
- Which combo of SATs are we using?
- Which type of tools should we use?
- Which cyber intel models should we use?

Intelligence Architecture Mind Map

Program (Managerial)

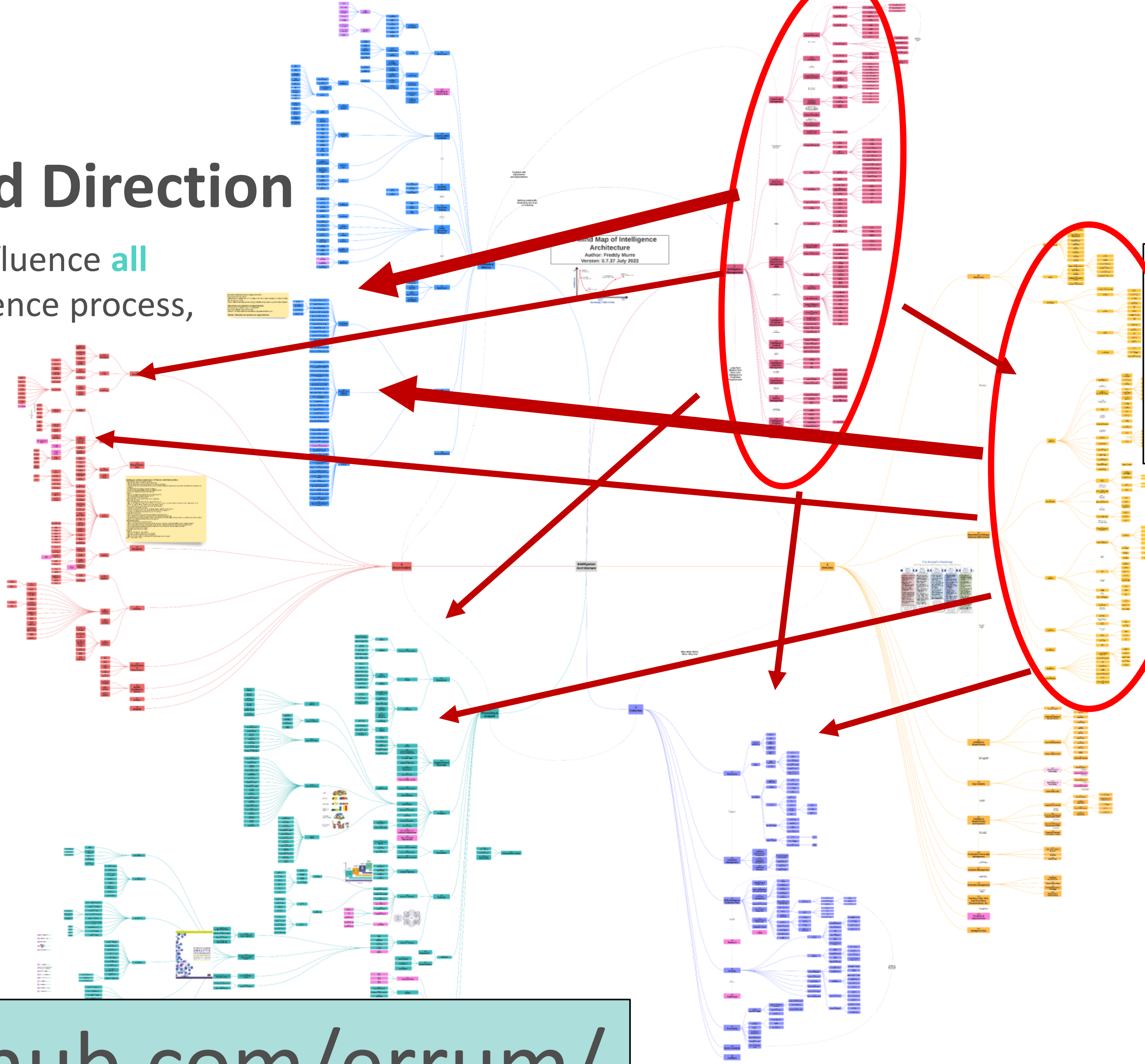


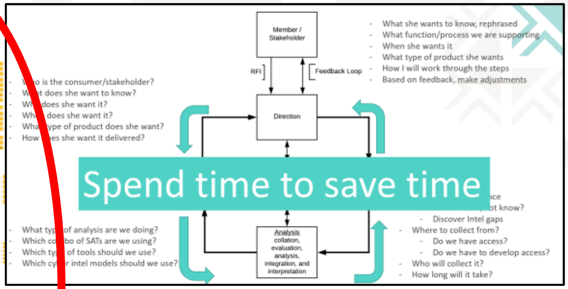
Process & Product

- Influenced by the Intelligence Cycle
- Six sections
  - Two program (managerial)
  - Four process and product
- Initially it is (intelligence) process-driven, THEN people and THEN Technology

Program and Direction

Program and Direction influence **all** other steps in the intelligence process, **especially** feedback & Metrics




Member / Stakeholder
RFI
Feedback Loop
Direction
Analysis
collation, evaluation, analysis, integration, and interpretation

- Who is the consumer/stakeholder?
- What does she want to know?
- Why does she want it?
- When does she want it?
- What type of product does she want?
- How does she want it delivered?

- What she wants to know, rephrased
- What function/process we are supporting
- When she wants it
- What type of product she wants
- How I will work through the steps
- Based on feedback, make adjustments

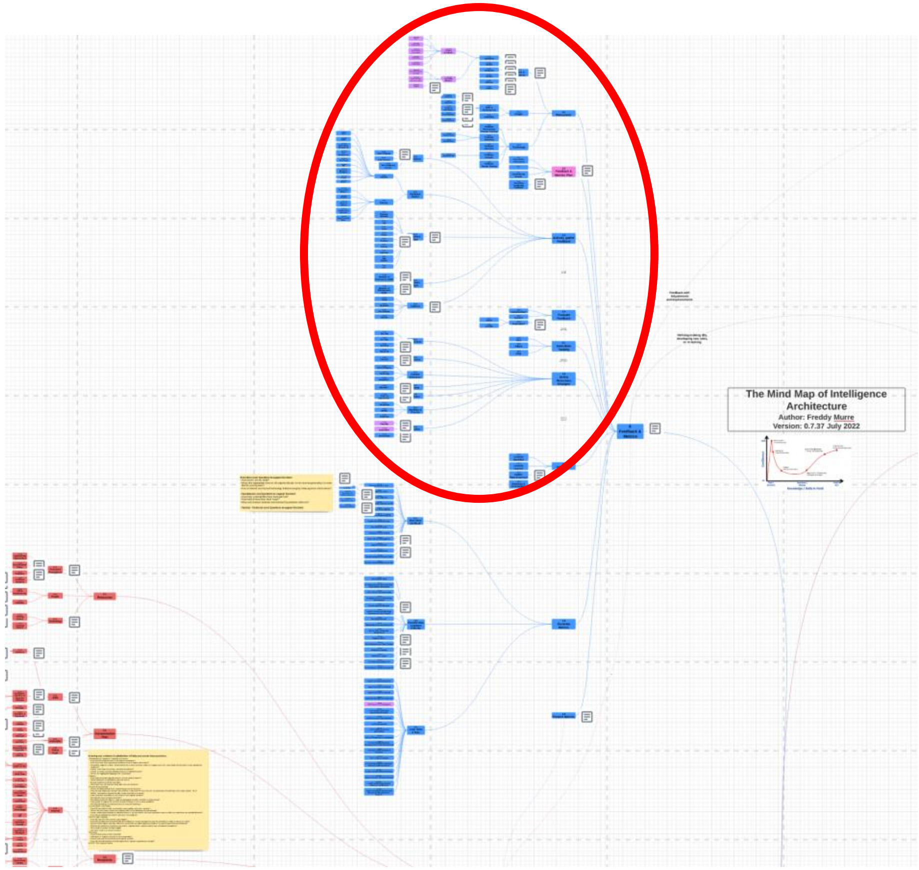
Spend time to save time

- What type of analysis are we doing?
- Which combo of SATs are we using?
- Which type of tools should we use?
- Which cyber intel models should we use?

nce
ot know?
  - Discover Intel gaps
- Where to collect from?
  - Do we have access?
  - Do we have to develop access?
- Who will collect it?
- How long will it take?

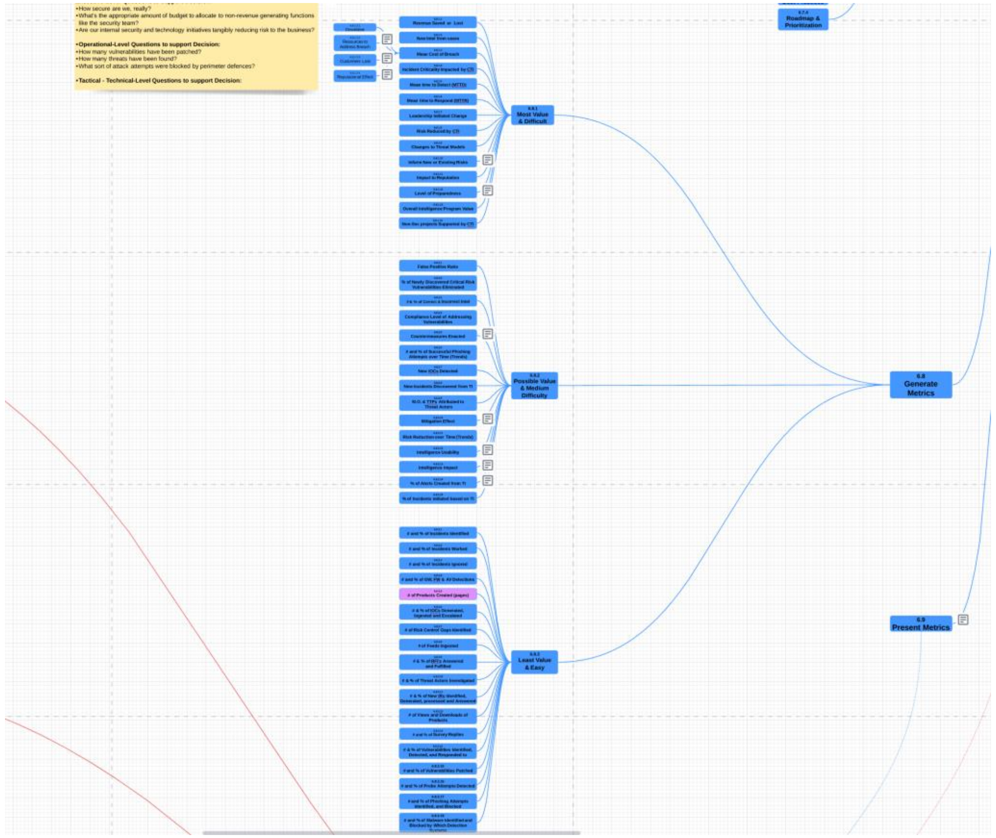
https://github.com/errum/

Intelligence Architecture Mind Map


The Mind Map of Intelligence Architecture
Author: Freddy Murre
Version: 0.7.37 July 2022

- Feedback & Metrics
- Based on input from the Cybersecurity community
- First part describes the steps/process

Intelligence Architecture Mind Map



- How secure are we, really?
- What's the appropriate amount of budget to allocate to non-revenue generating functions like the security team?
- Are our internal security and technology initiatives tangibly reducing risk to the business?

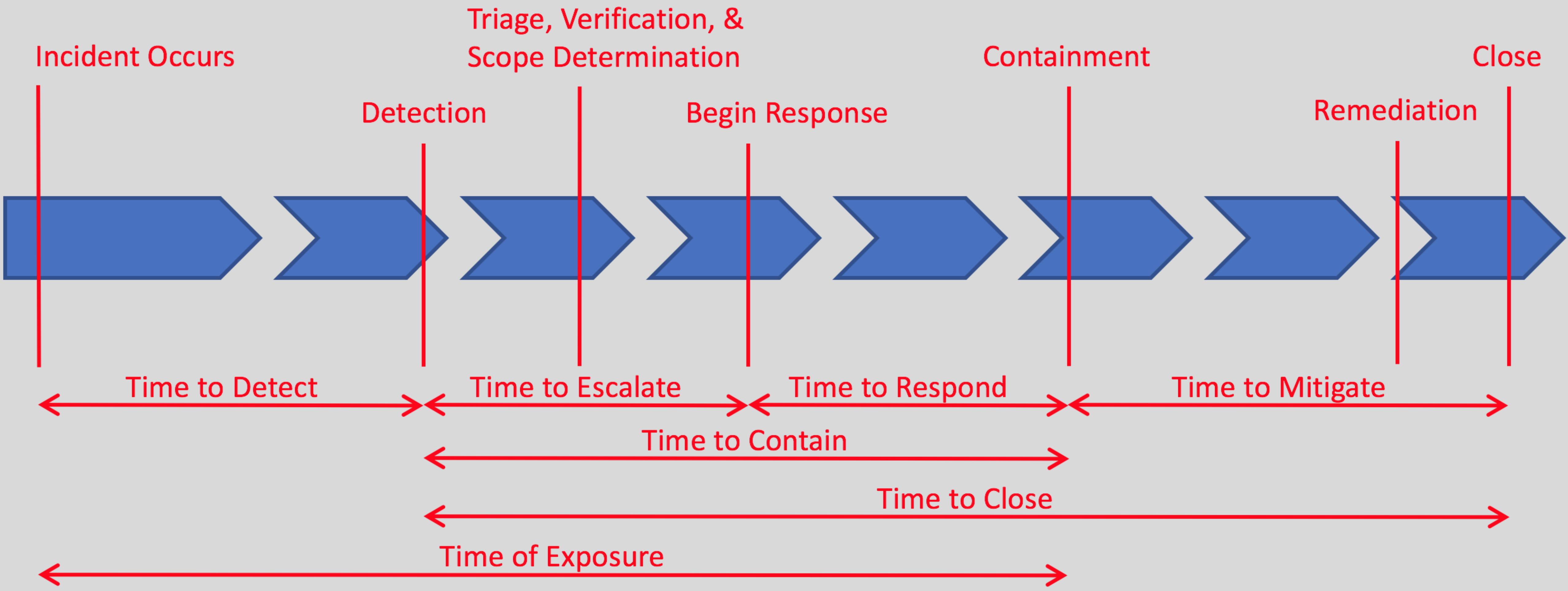
Operational-Level Questions to support Decision:

- How many vulnerabilities have been patched?
- How many threats have been found?
- What sort of attack attempts were blocked by perimeter defences?

Tactical - Technical-Level Questions to support Decision:

Downtime
Resources to Address Breach
Customers Lost
Reputational Effect
Revenue Saved or Lost
New Intel from cases
Mean Cost of Breach
Incident Criticality Impacted by CTI
Mean time to Detect (MTTD)
Mean time to Respond (MTTR)
Leadership Initiated Change
Risk Reduced by CTI
Changes to Threat Models
Inform New or Existing Risks
Impact to Reputation
Level of Preparedness
Overall Intelligence Program Value
New Sec projects Supported by CTI
Most Value & Difficult
Roadmap & Prioritization
False Positive Ratio
% of Newly Discovered Critical Risk Vulnerabilities Eliminated
# & % of Correct & Incorrect Intel
Compliance Level of Addressing Vulnerabilities
Countermeasures Enacted
# and % of Successful Phishing Attempts over Time (Trends)
New IOCs Detected
New Incidents Discovered from TI
M.O. & TTPs Attributed to Threat Actors
Mitigation Effect
Risk Reduction over Time (Trends)
Intelligence Usability
Intelligence Impact
% of Alerts Created from TI
% of Incidents initiated based on TI
Possible Value & Medium Difficulty
Generate Metrics
Present Metrics
# and % of Incidents Identified
# and % of Incidents Worked
# and % of Incidents Ignored
# and % of DW, FW & AV Detections
# of Products Created (pages)
# & % of IOCs Generated, Ingested and Escalated
# of Risk Control Gaps Identified
# of Feeds Ingested
# & % of RFI's Answered and Fulfilled
# & % of Threat Actors Investigated
# & % of New IRs Identified, Generated, processed and Answered
# of Views and Downloads of Products
# and % of Survey Replies
# & % of Vulnerabilities Identified, Detected, and Responded to
# and % of Vulnerabilities Patched
# and % of Probe Attempts Detected
# and % of Phishing Attempts Identified, and Blocked
# and % of Malware Identified and Blocked by Which Detection Systems
Least Value & Easy

- Second part helps identify and generate metrics of value
- Divided into three parts
  - Least Value, but easy
  - Possible value, medium difficulty
  - Most Value, but difficult



Source: https://www.taksati.org/metrics-that-matter/

Closing thoughts

The “right” metrics will depend on your industry, organization's needs, regulations, guidelines, best practices and ultimately, you and your stakeholders’ appetite for risk

- Abi Tunggal

Thank You