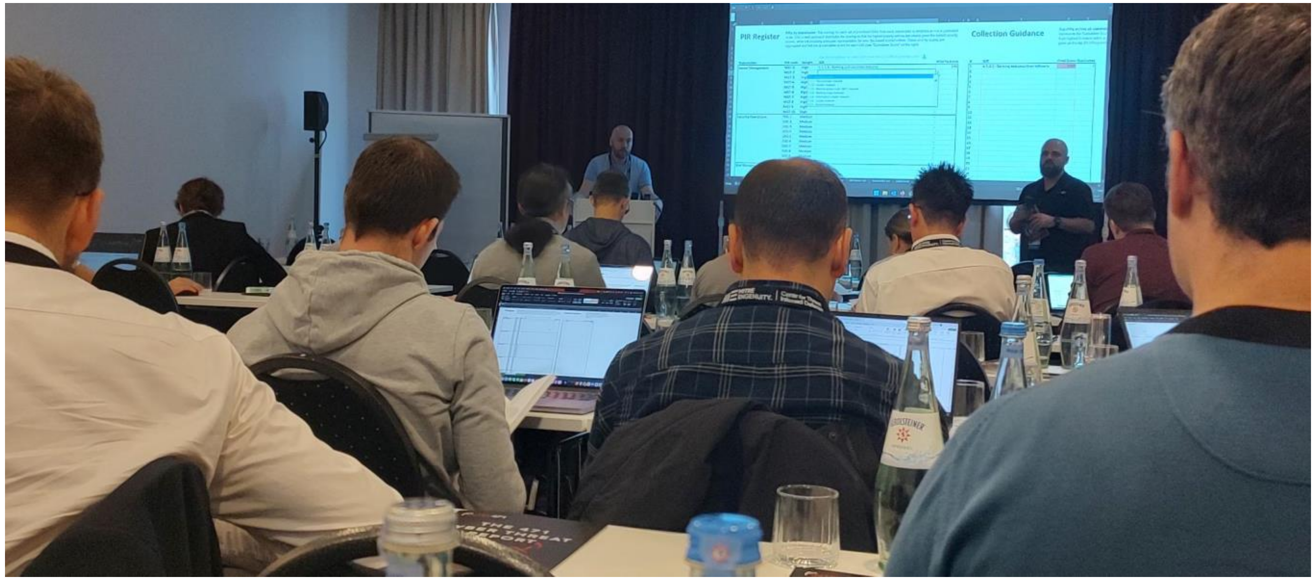
Foresight analysis:
The magic eight ball of intelligence analysis

FIRST CTI, Berlin - November, 2023

Establishing PIRs in Cyber
Ondra and Vladimir



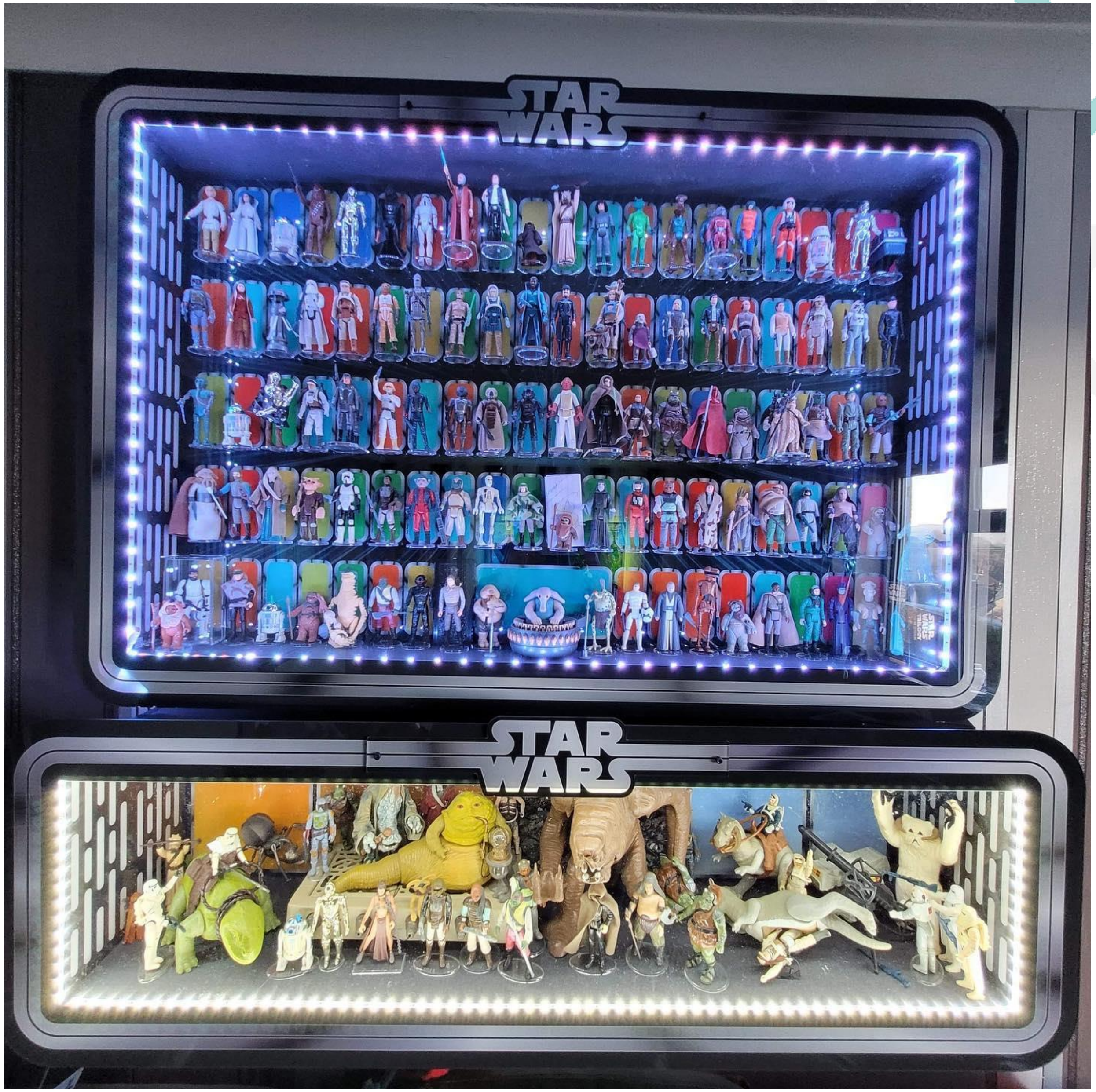
IRM for Cyber
Michael, Garret and Freddy

How to Align CTI and Risk
Jamie, John, and Grace

WhoAmI

– That's All I'll Ever Be

- Freddy M, Senior Advisor Threat Intelligence @ NFCERT
  - Focus on the operational level
  - Support strategic and tactical Level
- Intelligence in the Norwegian Army
- Education
  - BA in Marketing
  - MA in Counter Terrorism
  - MA in Intelligence



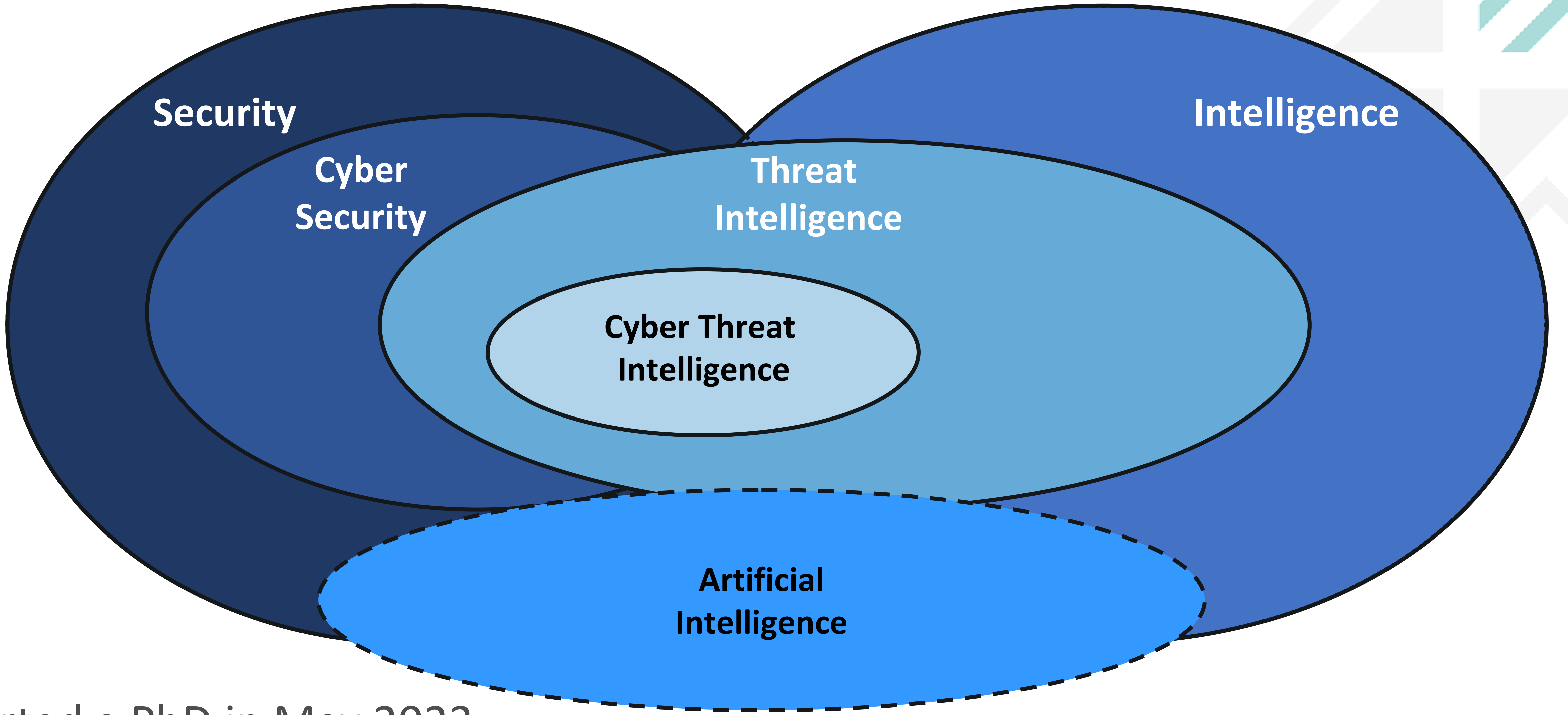
Agenda

– What happens, happens

- Introducing the Problem
- The start of a Solution
- The Experiment
- The Next Steps

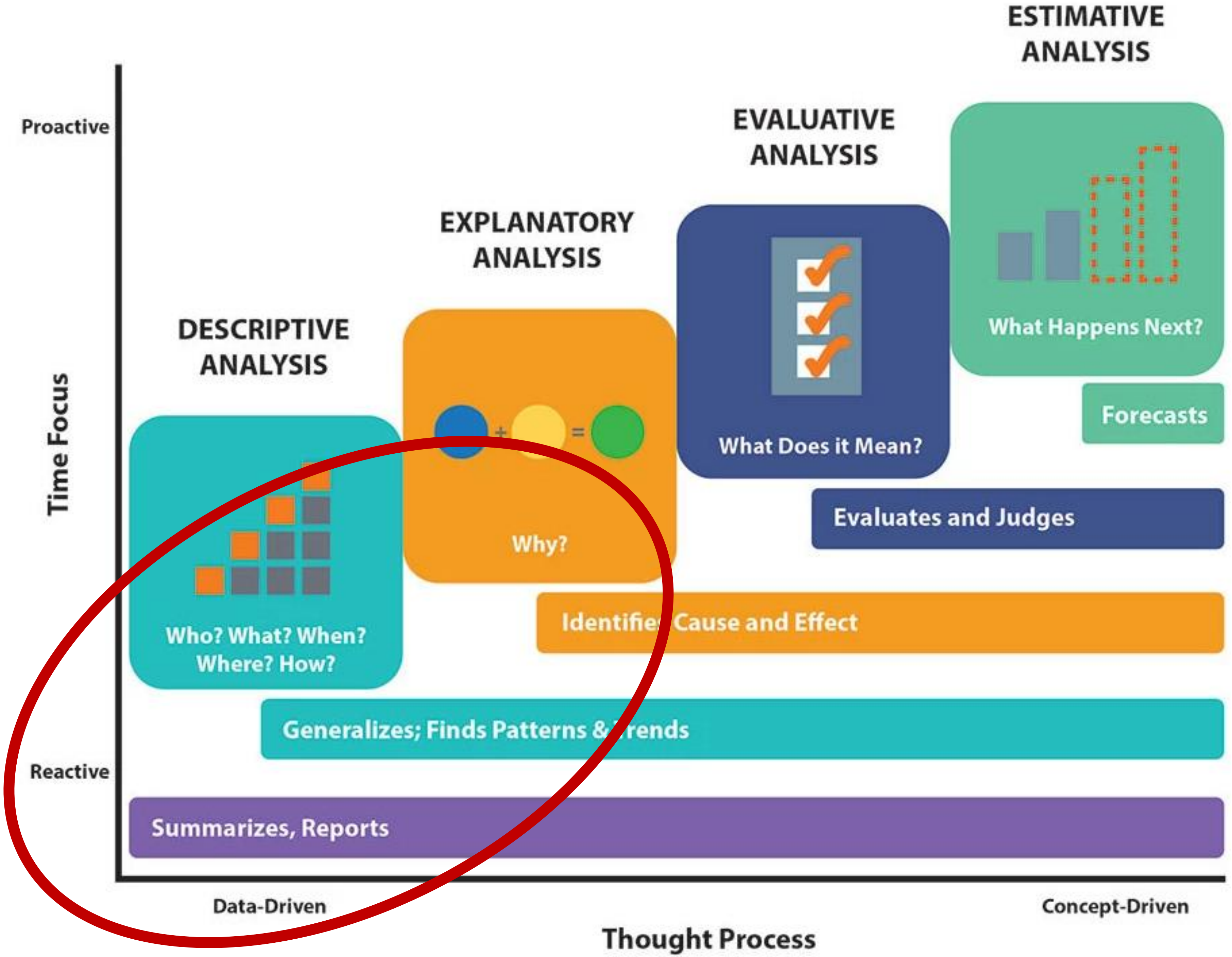
The “Problem”

Talking Intelligence to CTI folks



Started a PhD in May 2023

Researching the cross-section of intelligence tradecraft, CTI, and AI



ESTIMATIVE ANALYSIS

EVALUATIVE ANALYSIS

EXPLANATORY ANALYSIS

DESCRIPTIVE ANALYSIS

Proactive

Time Focus

Reactive

Who? What? When? Where? How?

Why?

What Does it Mean?

What Happens Next?

Forecasts

Evaluates and Judges

Identifies Cause and Effect

Generalizes; Finds Patterns & Trends

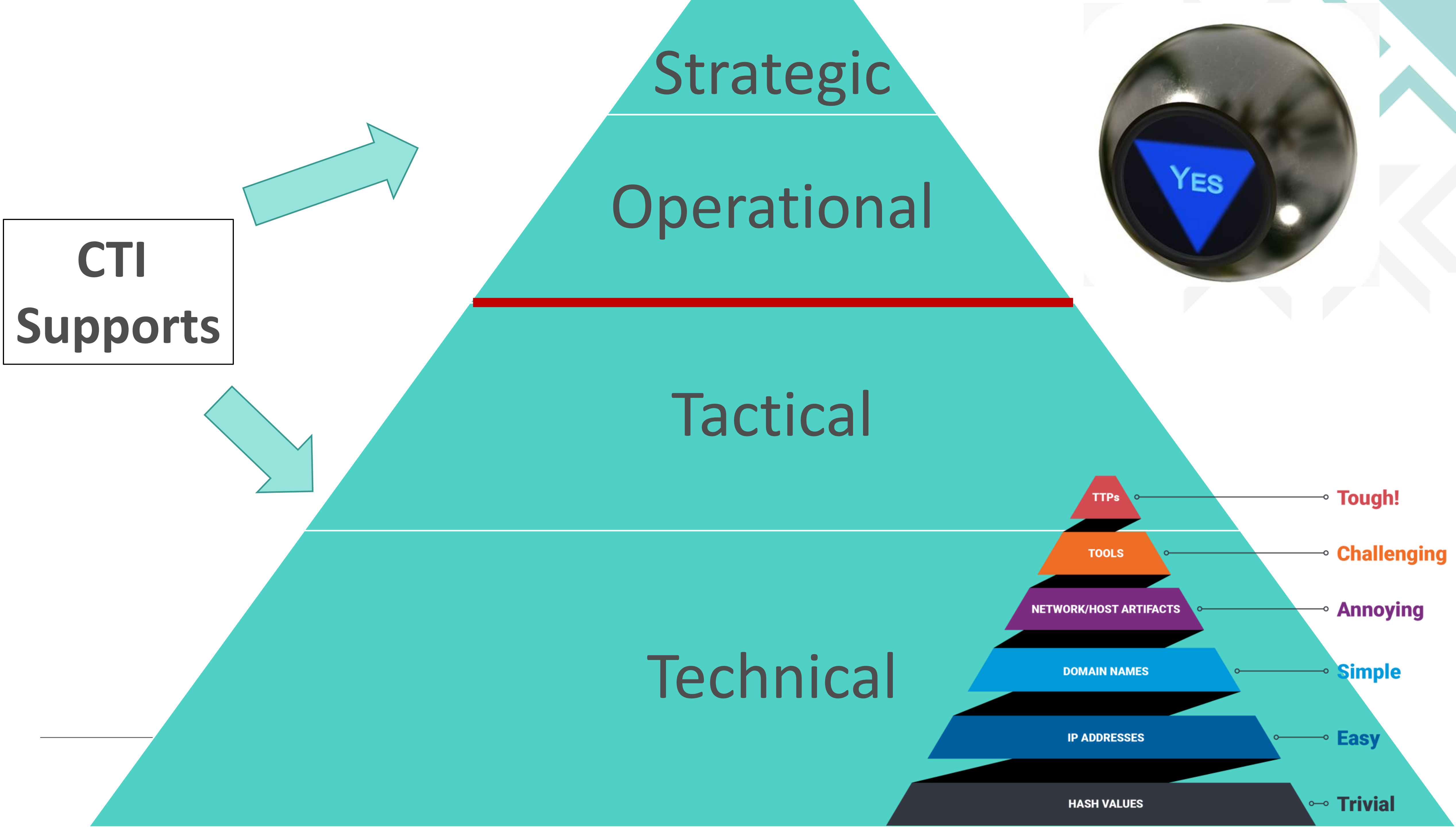
Summarizes, Reports

Data-Driven

Concept-Driven

Thought Process

MAGIC 8-BALL, AM I STUPID?



CTI Supports

Strategic

Operational

Tactical

Technical

The environment we work in has changed

- Increase in number & complexity of questions from the rest of the org, often from “higher up”
  - Completely different questions and focus
  - Money and risk versus malware analysis, data logs, and DDoS
- Focus on
  - The Org → Future risks
  - CTI → What the threat landscape will look like tomorrow

- Not knowing how to do foresight analysis
  - Support future decisions
- Risk and costs drives decisions

Conclusion

- CTI need to be able to support in futures analysis and assessments

The Start of a Solution

Collaborative CTI Groups

- Nordic → NFCERT-TIC
  - Threat Intelligence Committee
- Norway → TIC/TAC-NO
  - Threat Intelligence Committee AND Threat Analysis Committee
- Denmark→ TIC/TAC-DK
  - Threat Intelligence Committee AND Threat Analysis Committee

The Goals of TIC

- Already got Tactical and Technical levels covered
- Increase focus on operational and strategic Threat Intelligence (TI)
- Share knowledge, approaches, solutions, and “best practices”
- Seamless CTI collaboration on incidents, across countries and sectors

The Goals of TAC

- Learn about analytical tools, methodology, vocabulary, and approach
- Sharing their experiences (good and bad)
- Taking new skills back to the organisation

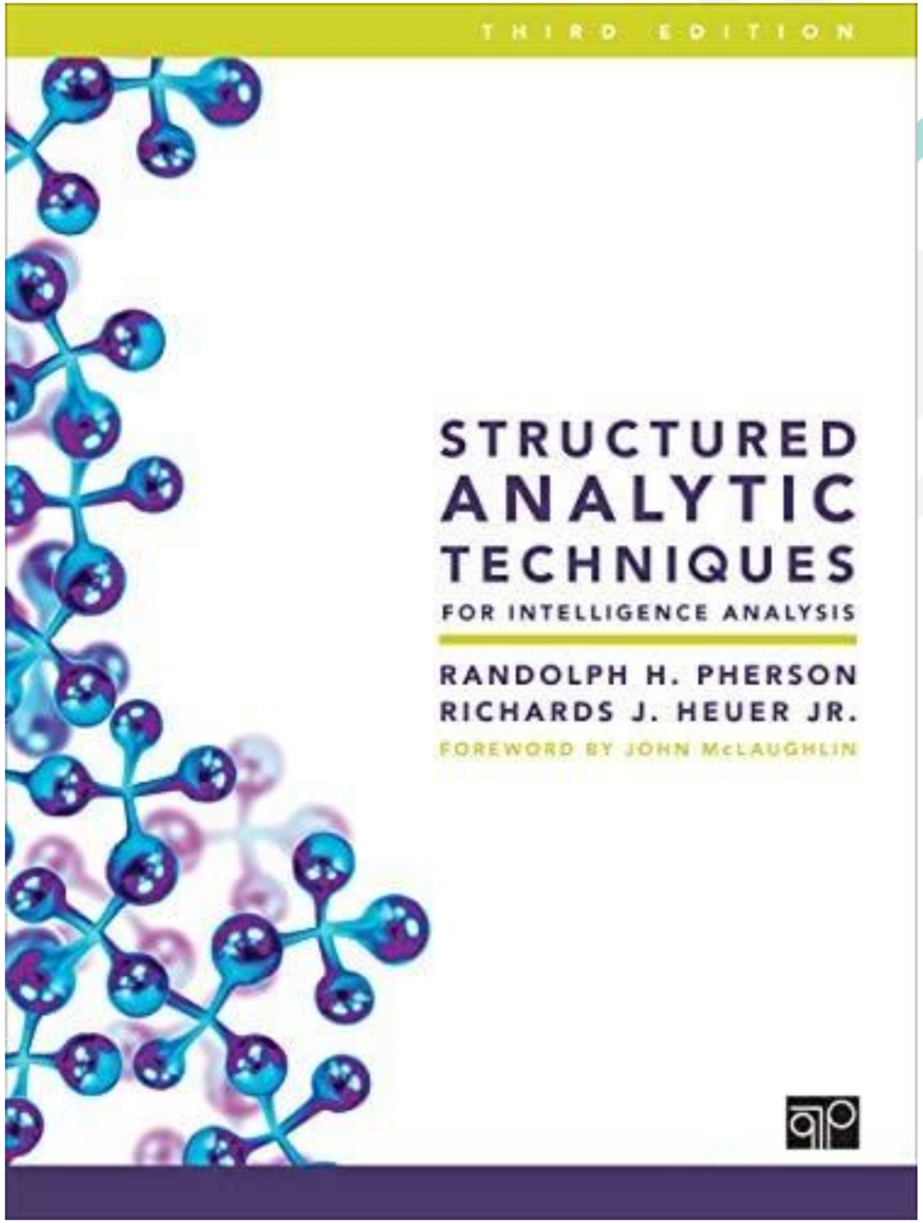
TIC-TAC

- 20+ member in each country
- Seasoned CTI professionals
- Cross-sectorial
- Meet several times a year
  - Mostly physical meetings
- Dedicated time for TIC and TAC subjects

- Cannot waste time getting everyone up to speed during an incidents
- How can we be more prepared for what may hit us?
- **Chosen focus**:
  - Structured Analytic Techniques (SATs)
- **End Goal:**
  - Foresight Analysis

Key Benefits of using SATs

- Externalise your thinking
- Identifying and Reducing Bias
- Reduce analytical errors
- Solving complex problems collaboratively
- Our biases, the problem, and the goal suggests the techniques to use
- The more we do them, the faster it will go


THIRD EDITION
STRUCTURED ANALYTIC TECHNIQUES
FOR INTELLIGENCE ANALYSIS
RANDOLPH H. PHERSON
RICHARDS J. HEUER JR.
FOREWORD BY JOHN McLAUGHLIN

Bias & Heuristics

– Your true colours shining through

KEY CHARACTERISTICS

- Quick to form

Highly resistant to change

Information is made to fit into an existing conceptual framework

We don’t see new patterns emerging

Initial, incorrect perceptions persist even after better information is available

We ignore or dismiss outlier data as noise

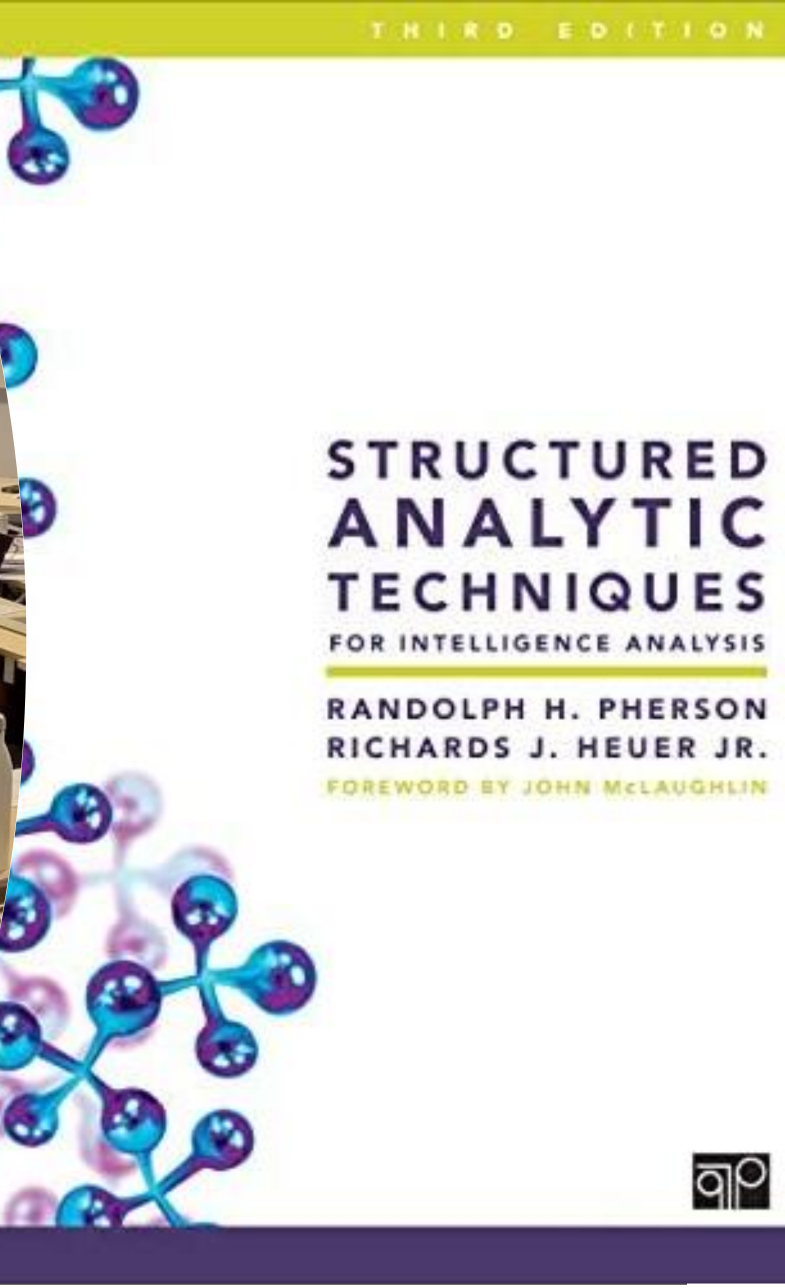
The Experiment

SATs and Intelligence tradecraft training

Teaching

- Intelligence analysis
- Critical thinking
- Structured Analytical Techniques (SAT)
- Disseminating finished intelligence

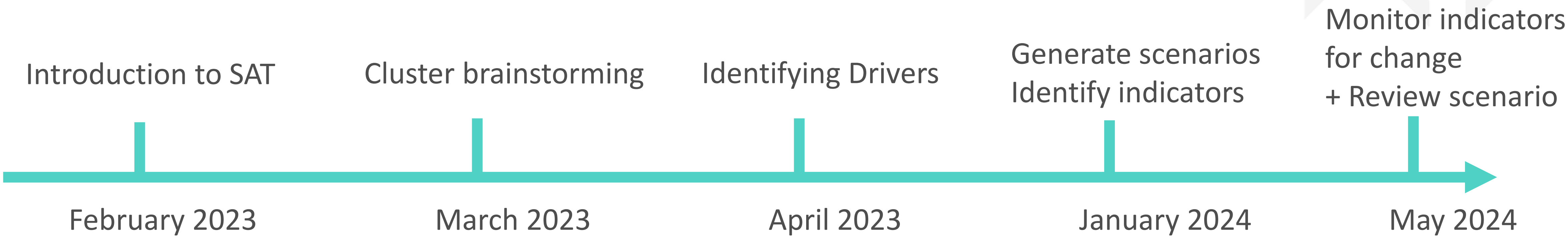
to the wider cyber security community


THIRD EDITION
STRUCTURED ANALYTIC TECHNIQUES
FOR INTELLIGENCE ANALYSIS
RANDOLPH H. PHERSON
RICHARDS J. HEUER JR.
FOREWORD BY JOHN McLAUGHLIN

Spend time to save time

SAT for foresight analysis

Timeline



Introduction to SAT

February 2023

Cluster brainstorming

March 2023

Identifying Drivers

April 2023

Generate scenarios
Identify indicators

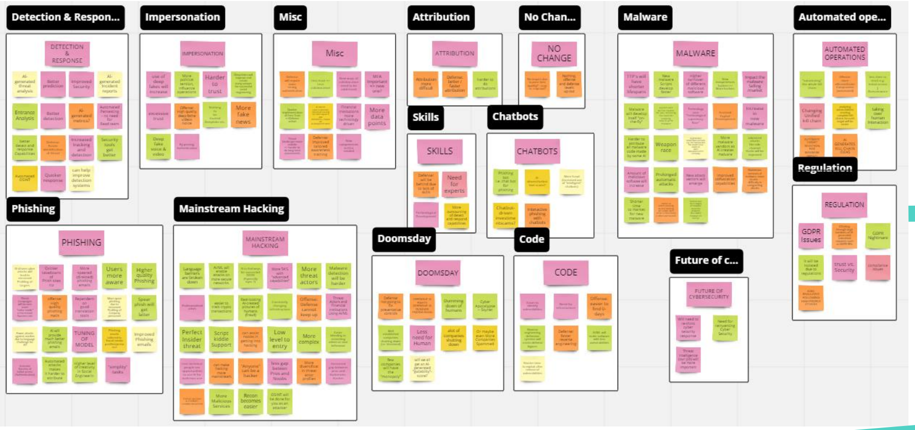
January 2024

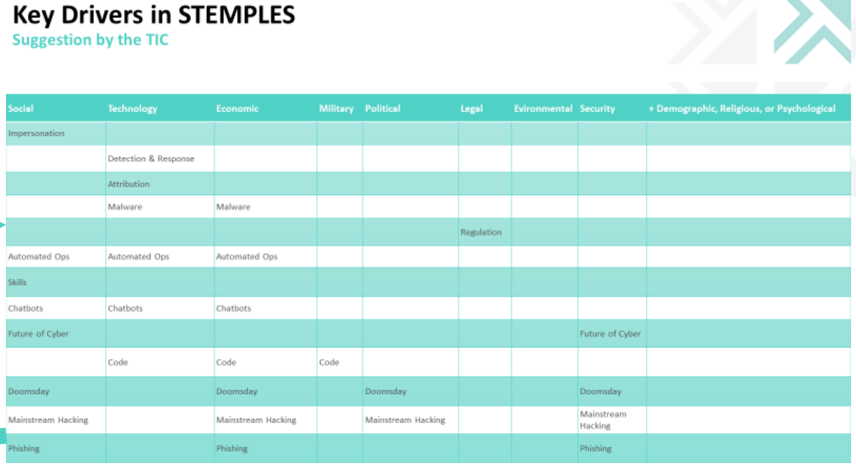
Monitor indicators
for change
+ Review scenario

May 2024

SATs & foresight analysis

How can AI and ML, and its influence in cybersecurity, change the Nordic financial sector’s threat landscape the coming three years?

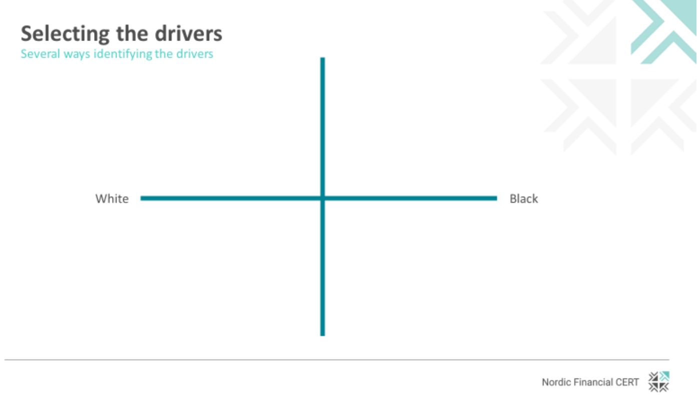




Key Drivers in STEMPLES

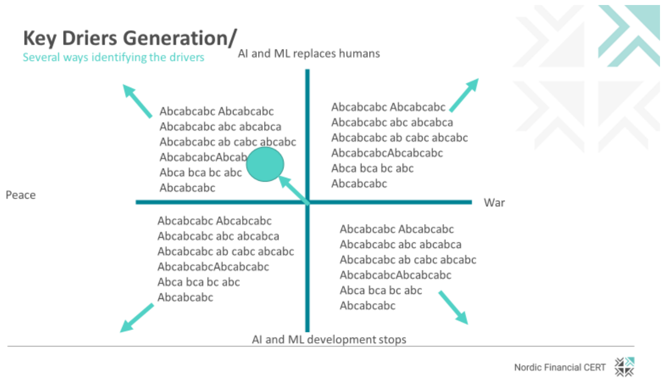
Suggestion by the TIC

Social	Technology	Economic	Military	Political	Legal	Evironmental	Security	+ Demographic, Religious, or Psychological
Impersonation								
	Detection & Response							
	Attribution							
	Malware	Malware						
					Regulation			
Automated Ops	Automated Ops	Automated Ops						
Skills								
Chatbots	Chatbots	Chatbots						
Future of Cyber							Future of Cyber	
	Code	Code	Code					
Doomsday		Doomsday		Doomsday			Doomsday	
Mainstream Hacking		Mainstream Hacking		Mainstream Hacking			Mainstream Hacking	
Phishing		Phishing					Phishing	



Selecting the drivers

Several ways identifying the drivers



Key Driers Generation/

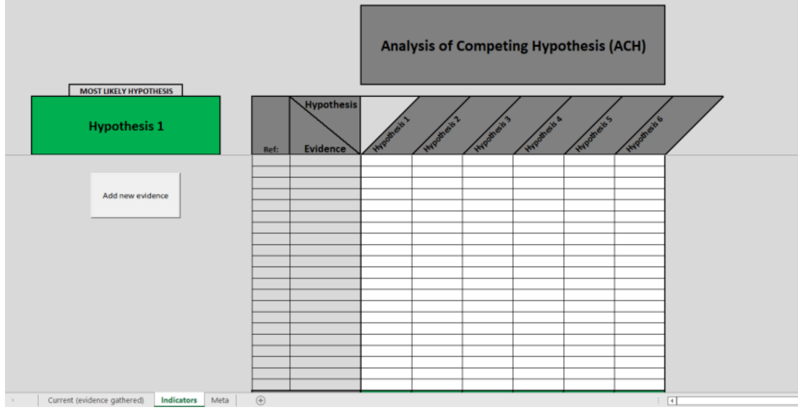
Several ways identifying the drivers

Abcabcabc Abcabcabc
Abcabcabc abc abcabca
Abcabcabc ab cabc abcabc
AbcabcabcAbcabcabc
Abca bca bc abc
Abcabcabc

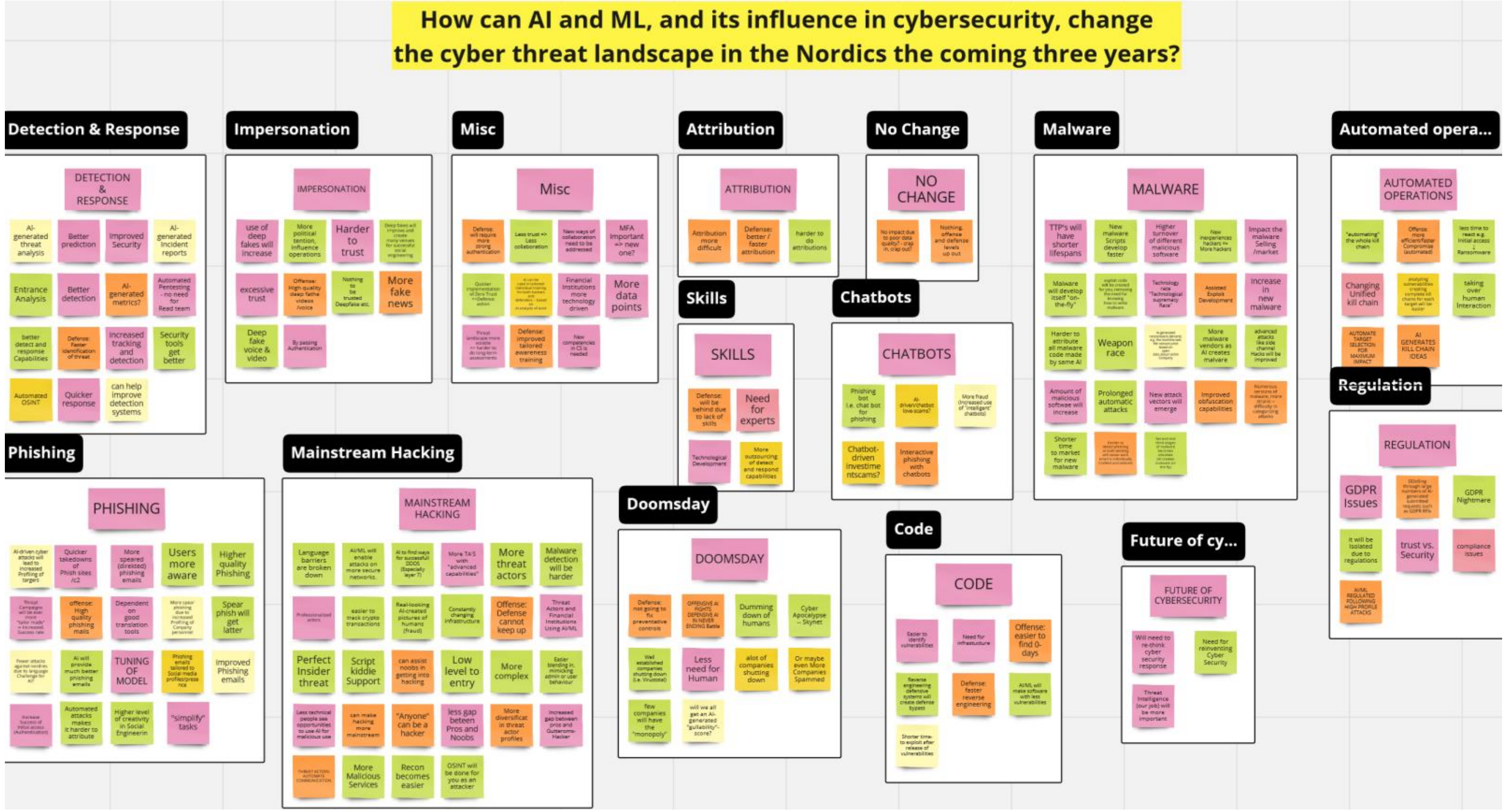
Abcabcabc Abcabcabc
Abcabcabc abc abcabca
Abcabcabc ab cabc abcabc
AbcabcabcAbcabcabc
Abca bca bc abc
Abcabcabc

Abcabcabc Abcabcabc
Abcabcabc abc abcabca
Abcabcabc ab cabc abcabc
AbcabcabcAbcabcabc
Abca bca bc abc
Abcabcabc

Abcabcabc Abcabcabc
Abcabcabc abc abcabca
Abcabcabc ab cabc abcabc
AbcabcabcAbcabcabc
Abca bca bc abc
Abcabcabc

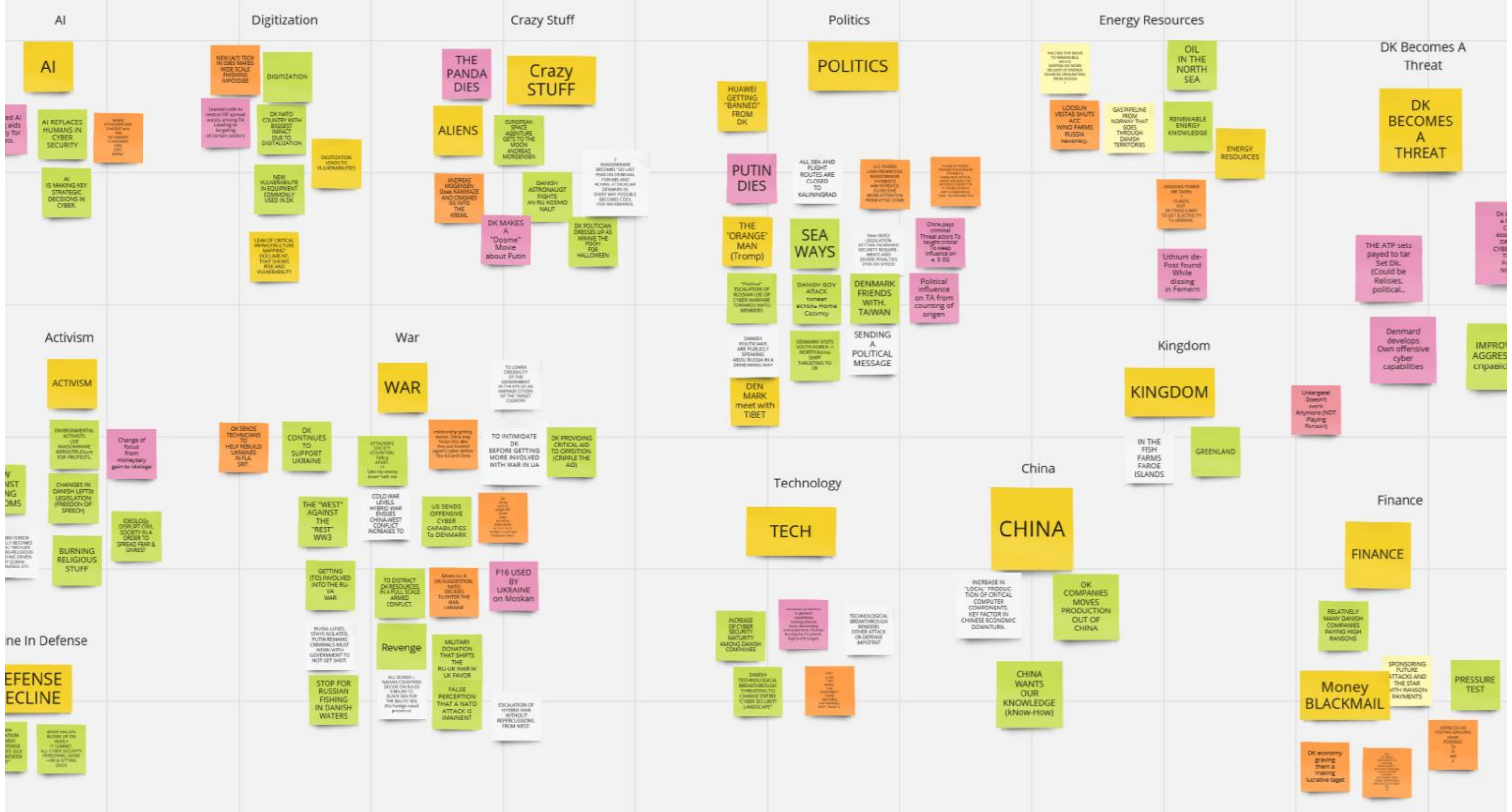


TIC-TAC-NO - Foresight Project


How can AI and ML, and its influence in cybersecurity, change the cyber threat landscape in the Nordics the coming three years?
Detection & Response
DETECTION & RESPONSE
AI-generated threat analysis
Better prediction
Improved Security
AI-generated Incident reports
Entrance Analysis
Better detection
AI-generated metrics?
Automated Pentesting - no need for Read team
better detect and response Capabilities
Defense: Faster identification of threat
Increased tracking and detection
Security tools get better
Automated OSINT
Quicker response
can help improve detection systems
Impersonation
IMPERSONATION
use of deep fakes will increase
More political tention, influence operations
Harder to trust
excessive trust
Offense: High quality deep fathe videos /voice
Nothing to be trusted Deepfake etc.
More fake news
Deep fake voice & video
By passing Authentication
Misc
Defense: will require more strong authentication
Less trust => Less collaboration
New ways of collaboration need to be addressed
MFA Important => new one?
Quicker implementation of Zero Trust =>Defense action
Financial Institutions more technology driven
More data points
Defense: improved tailored awereness training
New competencies in CS is needed
Attribution
ATTRIBUTION
Attribution more difficult
Defense: better / faster attribution
harder to do attributions
No Change
NO CHANGE
No impact due to poor data quality? - crap in, crap out?
Nothing, offense and defense levels up out
Skills
SKILLS
Defense: will be behind due to lack of skills
Need for experts
Technological Development
More outsourcing of detect and respond capabilities
Chatbots
CHATBOTS
Phishing bot i.e. chat bot for phishing
AI-driven/chatbot love-scams?
More fraud (increased use of "intelligent" chatbots)
Chatbot-driven investimentscams?
Interactive phishing with chatbots
Malware
MALWARE
TTP's will have shorter lifespans
New malware Scripts develop faster
Higher turnover of different malicious software
New inexperiences hackers => More hackers
Impact the malware Selling /market
Malware will develop itself "on-the-fly"
Technology race "Technological supremacy Race"
Assisted Exploit Development
Increase in new malware
Harder to attribute all malware code made by same AI
Weapon race
More malware vendors as AI creates malware
advanced attacks like side channel Hacks will be improved
Amount of malicious softwae will increase
Prolonged automatic attacks
New attack vectors will emerge
Improved obfuscation capabilities
Shorter time to market for new malware
Automated opera...
AUTOMATED OPERATIONS
"automating" the whole kill chain
Offense: more efficient/faster Compromise (automated)
less time to react e.g. Initial access ↓ Ransomware
Changing Unified kill chain
taking over human Interaction
AUTOMATE TARGET SELECTION FOR MAXIMUM IMPACT
AI GENERATES KILL CHAIN IDEAS
Regulation
REGULATION
GDPR Issues
GDPR Nightmare
it will be isolated due to regulations
trust vs. Security
compliance issues
AI/ML REGULATED FOLLOWING HIGH PROFILE ATTACKS
Phishing
PHISHING
AI-driven cyber attacks will lead to increased Profiling of targers
Quicker takedowns of Phish sites /c2
More speared (direkted) phishing emails
Users more aware
Higher quality Phishing
offense: High quality phishing mails
Dependent on good translation tools
Spear phish will get latter
AI will provide much better phishing emails
TUNING OF MODEL
Phishing emails tailored to Social media profiles/presence
Improved Phishing emails
Automated attacks makes it harder to attribute
Higher level of creativity in Social Engineerin
"simplify" tasks
Mainstream Hacking
MAINSTREAM HACKING
Language barriers are broken down
AI/ML will enable attacks on more secure networks.
AI to find ways for successfull DDOS (Especialy layer 7)
More TA'S with "advanced capabilities"
More threat actors
Malware detection will be harder
easier to track crypto transactions
Real-looking AI-created pictures of humans (fraud)
Constantly changing infrastructure
Offense: Defense cannot keep up
Threat Actors and Financial Institutions Using AI/ML
Perfect Insider threat
Script kiddie Support
can assist noobs in getting into hacking
Low level to entry
More complex
Easier blending in, mimicking admin or user behaviour
Less technical people see opportunities to use AI for malicious use
can make hacking more mainstream
"Anyone" can be a hacker
less gap beteen Pros and Noobs
More diversificat in threat actor profiles
Increased gap between pros and Gutteroms-Hacker
More Malicious Services
Recon becomes easier
OSINT will be done for you as an attacker
Doomsday
DOOMSDAY
Defense: not going to fix preventative controls
OFFENSIVE AI FIGHTS DEFENSIVE AI IN NEVER ENDING Battle
Dumming down of humans
Cyber Apocalypse – Skynet
Well established companies shutting down (i.e. Virustotal)
Less need for Human
alot of companies shutting down
Or maybe even More Companies Spammed
few companies will have the "monopoly"
will we all get an AI-generated "gullability"-score?
Code
CODE
Easier to identify vulnerabilities
Need for infrastucture
Offense: easier to find 0-days
Reverse engineering defensive systems will create defense bypass
Defense: faster reverse engineering
AI/ML will make software with less vulnerabilities
Shorter time to exploit after release of vulnerabilities
Future of cy...
FUTURE OF CYBERSECURITY
Will need to re-think cyber security response
Need for reinventing Cyber Security
Threat Intelligence (our job) will be more important

- **Research Question:** How can AI and ML, and its influence in cybersecurity, change the cyber threat landscape in the Nordics the coming three years?

TIC-TAC-DK - Foresight Project



› **Research Question:** What would cause advanced threat actors to shift focus from "untargeted" ransomware attacks to targeting DK's critical infrastructure and its supply chain?

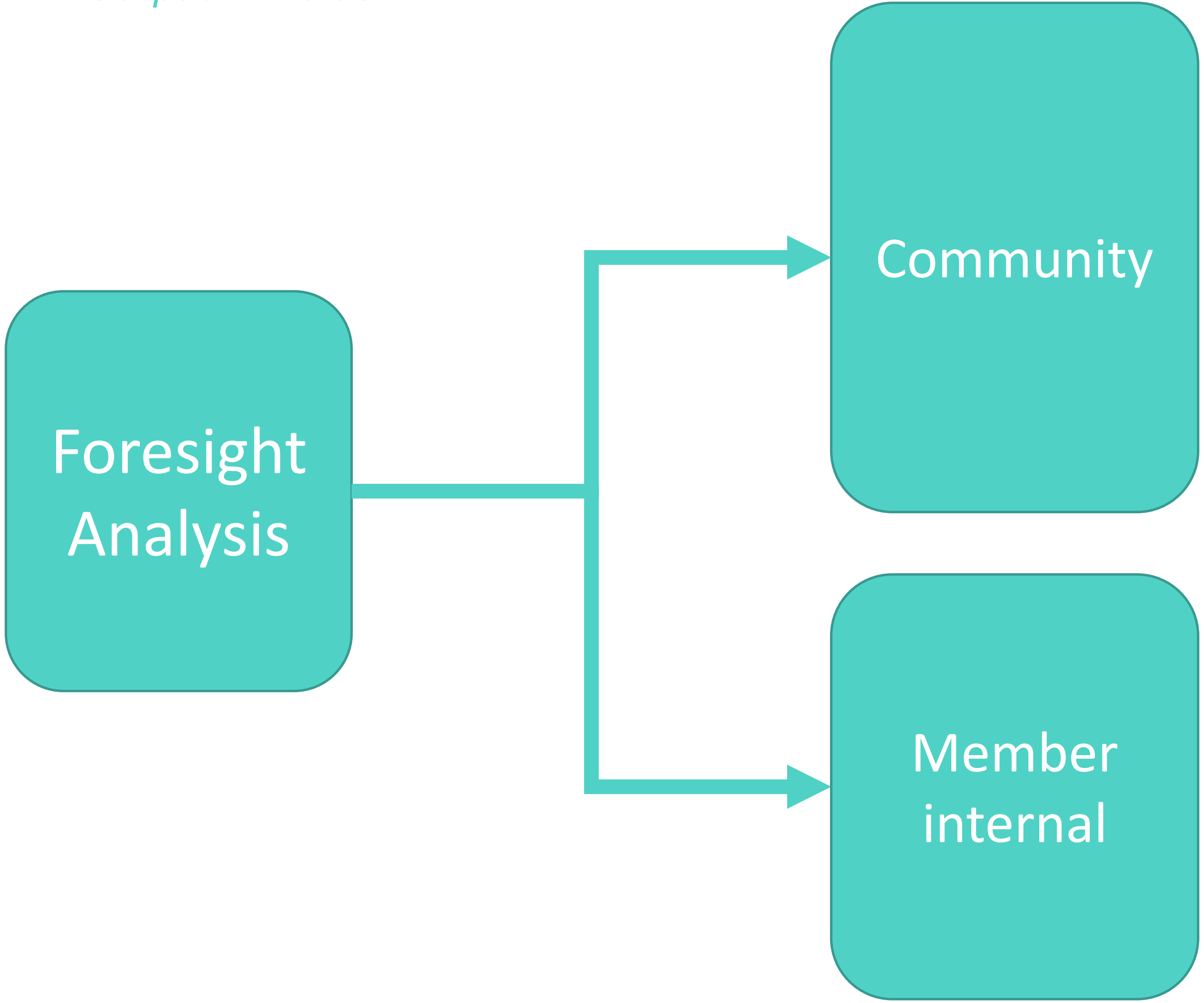
NFCERT TIC - Foresight Project

- **Research Question:**
  If the Russia-Ukraine war stops tomorrow/near future (conflict continues), how will this change the cyber threat landscape in the Nordics?

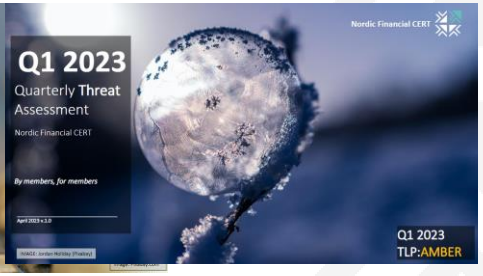
- **Underlying reasoning for all TIC/TACs**
  How do we prepare and budget for the future?

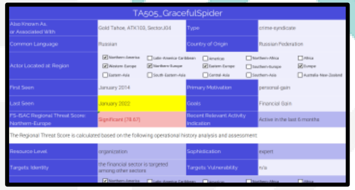
SATs & foresight analysis

Output → Value

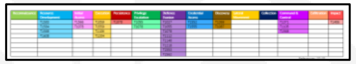


2023
Generic Threat Landscape
December 2022 v1.1
TLP:AMBER


Nordic Financial CERT
Q1 2023
Quarterly Threat Assessment
Nordic Financial CERT
By members, for members
April 2023 v.1.0
Q1 2023
TLP:AMBER


TA505_GracefulSpider

Also Known As or Associated With	Gold Tahoe, ATK103, SectorJ04	Type	crime-syndicate
Common Language	Russian	Country of Origin	Russian Federation
Actor Located at: Region	☑ Northern-America ☐ Latin-America-Caribbean ☐ Americas ☐ Northern-Africa ☐ Africa ☑ Western-Europe ☑ Northern-Europe ☑ Eastern-Europe ☐ Southern-Europe ☑ Europe ☐ Eastern-Asia ☐ South-Eastern-Asia ☐ Central-Asia ☐ Southern-Asia ☐ Australia-New-Zealand		
First Seen	January 2014	Primary Motivation	personal-gain
Last Seen	January 2022	Goals	Financial Gain
FS-ISAC Regional Threat Score: Northern-Europe	Significant (78.67)	Recent Relevant Activity Indication	Active in the last 6 months
The Regional Threat Score is calculated based on the following operational history analysis and assessment:			
Resource Level	organization	Sophistication	expert
Targets: Identity	the financial sector is targeted among other sectors	Targets: Vulnerability	n/a



Assessments → Foresight

Common Standard & Voice

Knowledge → Analysis

Improved internal products/Assessments

Internal foresight

Organizational learning

Results, so far

- Identified individual, team, organizational and vendors Biases
- Experience with a selection of SATs
- Critical thinking
- Daring to challenge prevailing views
- Reducing Bias
- Testing foresight analysis to enhance reports and communication

MAIN Goal

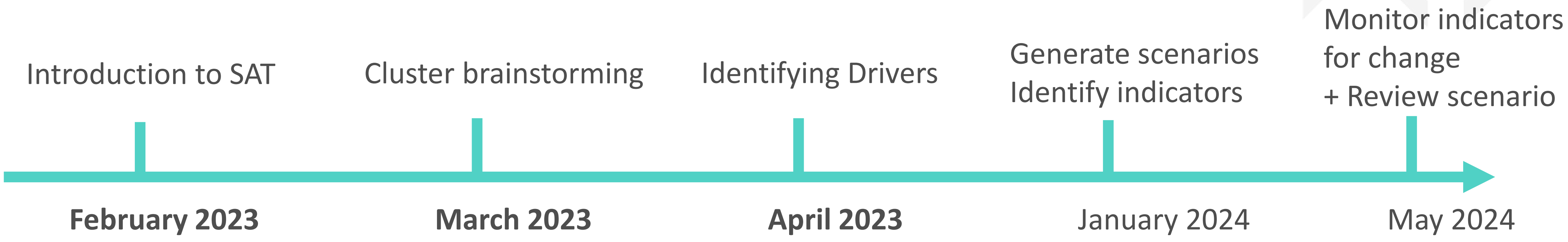
- Ensure the CTI function provides value beyond tactical & technical support

= get more funding, or at the very minimum, keep existing funding

The Next Steps

SAT for foresight analysis

Timeline



Introduction to SAT

February 2023

Cluster brainstorming

March 2023

Identifying Drivers

April 2023

Generate scenarios
Identify indicators

January 2024

Monitor indicators for change
+ Review scenario

May 2024

Foresight analysis and the Magic Eight Ball

- Forecast
- Foresight
- Futures Analysis
- Tea Leaves
- Fortune Telling
- Guesstimates

NOT a truth teller

- Support Assessments + Confidence

Support or Collaborate?

- **GitHub**: errum