Intelligence Preparation of the Cyber Environment

Rob Dartnall | Director
– Cyber Intelligence

Rob Dartnall

Director – Cyber Intelligence

Rob is a CREST Certified Threat Intelligence Manager (CCTIM) and Cyber Intelligence Director/CEO of Security Alliance - a Bank of England/DNB/HKMA certified Cyber Threat Intelligence provider under the CBEST/Tiber/iCAST frameworks. With specialist interest areas of Insider Threat and Nation State Fusion Warfare, Mr Dartnall has unique experience and insight into the threat landscape. In his role as the Associate Director of Cyber Threat Intelligence to Gartner, Rob and Security Alliance are the global providers of Threat Intelligence services to Gartner consulting.

From a conventional Military Intelligence background Mr Dartnall has been creating cyber threat assessments and building intelligence teams and testing programs for some of the largest organisations in Europe, North America, the Middle East and Africa.

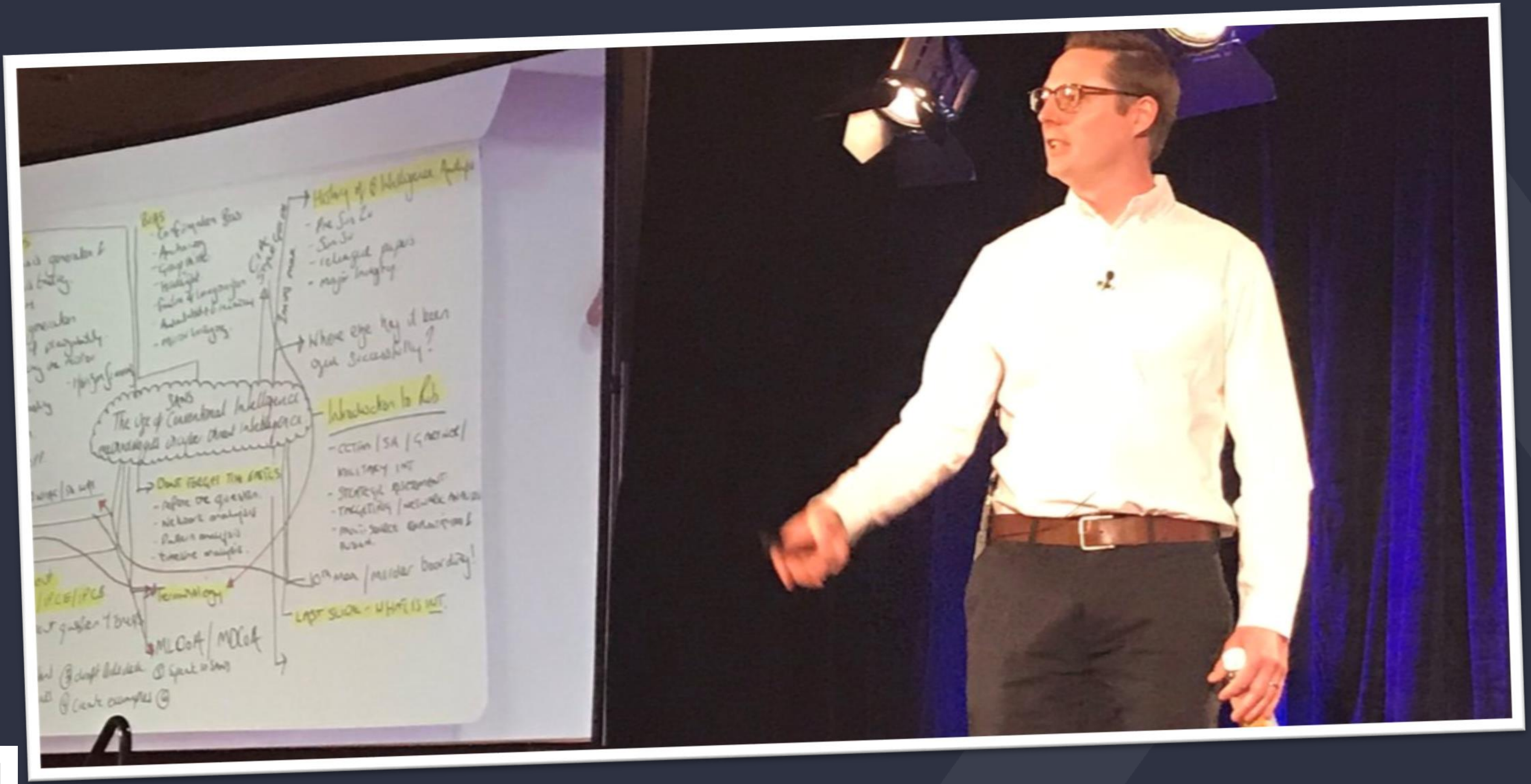
Rob Dartnall

Director – Cyber Intelligence

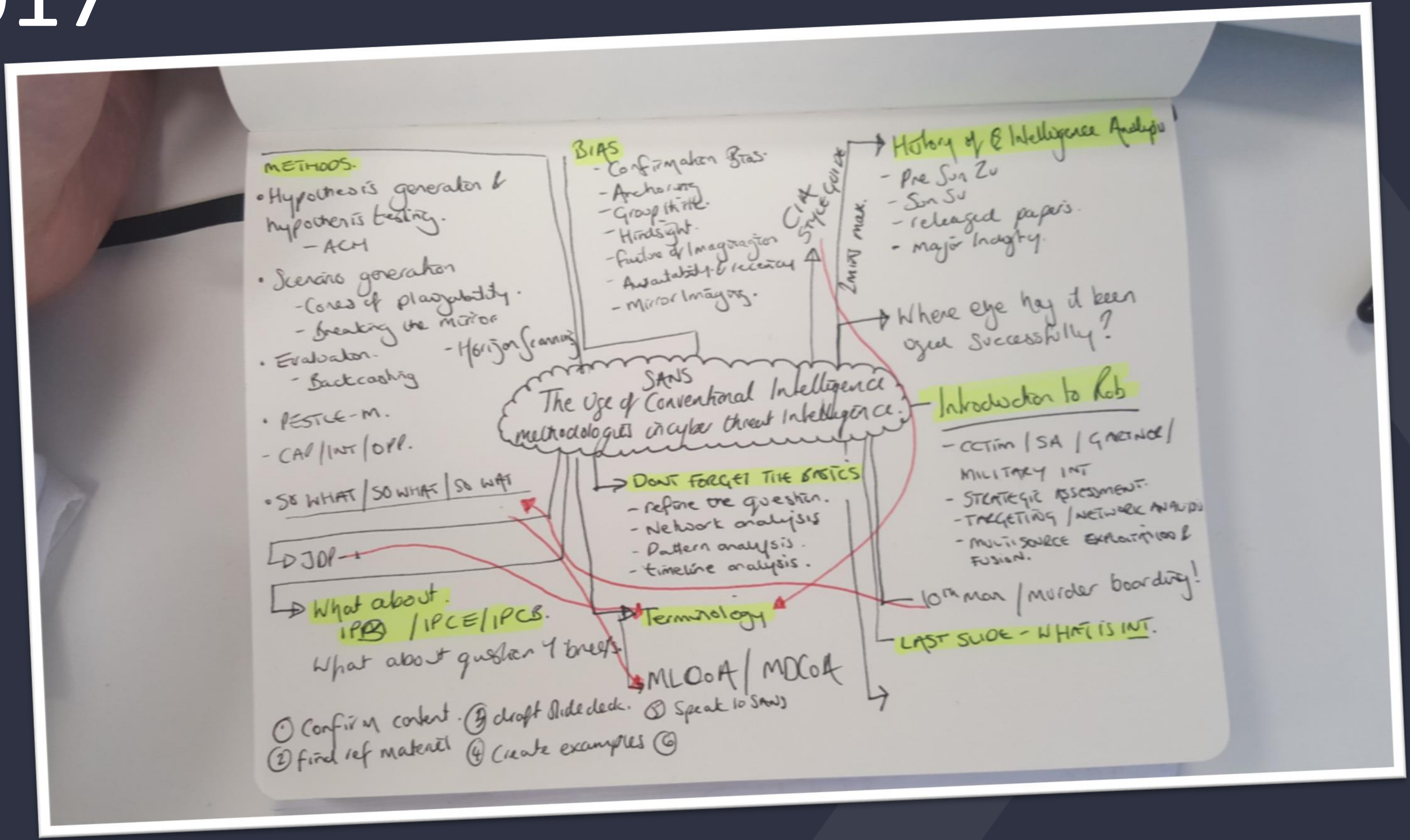
Rob is a **CREST Certified Threat Intelligence Manager (CCTIM)** and **Cyber Intelligence Director/CEO of Security Alliance - a Bank of England/DNB/HKMA** certified Cyber Threat Intelligence provider under the **CBEST/Tiber/ICAST** frameworks. With specialist interest areas of **Insider Threat** and **Nation State Fusion Warfare**, Mr Dartnall has unique experience and insight into the threat landscape. In his role as the **Associate Director of Cyber Threat Intelligence to Gartner**, Rob and Security Alliance are the global providers of Threat Intelligence services to Gartner consulting.

From a conventional Military Intelligence background Mr Dartnall has been **creating cyber threat assessments and building intelligence teams** and testing programs for some of the largest organisations in Europe, North America, the Middle East and Africa.

2017



2017


METHODS.
• Hypothesis generation & hypothesis testing.
– ACH
• Scenario generation
– Cones of plausability.
– Breaking the mirror
• Evaluation.
– Backcasting
– Horizon scanning
• PESTLE-M.
– CAP/INT/OPP.
• SO WHAT / SO WHAT / SO WHAT
BIAS
– Confirmation Bias.
– Anchoring
– Group think.
– Hindsight.
– Failure of Imagination
– Mirror Imaging.
CIA Style guide
2 mins max.
History of Intelligence Analysis
– Pre Sun Zu
– Sun Su
– released papers.
– major Inqiry.
Where else has it been used successfully?
SANS
The Use of Conventional Intelligence methodologies in cyber threat Intelligence.
Introduction to Rob
– CCTIM / SA / GARTNER /
MILITARY INT
– STRATEGIC ASSESSMENT.
– TARGETING / NETWORK ANALYSIS
– MULTISOURCE EXPLOITATION & FUSION.
DONT FORGET THE BASICS
– refine the question.
– Network analysis
– Pattern analysis.
– timeline analysis.
JDP
What about IPB / IPCE / IPCB.
What about question 1 brief.
Terminology
MLCoA / MDCoA
10th man / murder boarding!
LAST SLIDE – WHAT IS INT.
① Confirm content
② Find ref material
③ draft slide deck.
④ Create examples
⑤ Speak to SANS
⑥

THE BRIEFEST HISTORY OF INTELLIGENCE YOU WILL EVER SEE...





MURDER BOARD

*are used to aggressively review, **without constraint or pleasantries**, a lem, assumptions, constraints, mitigations, and the proposed solution.*

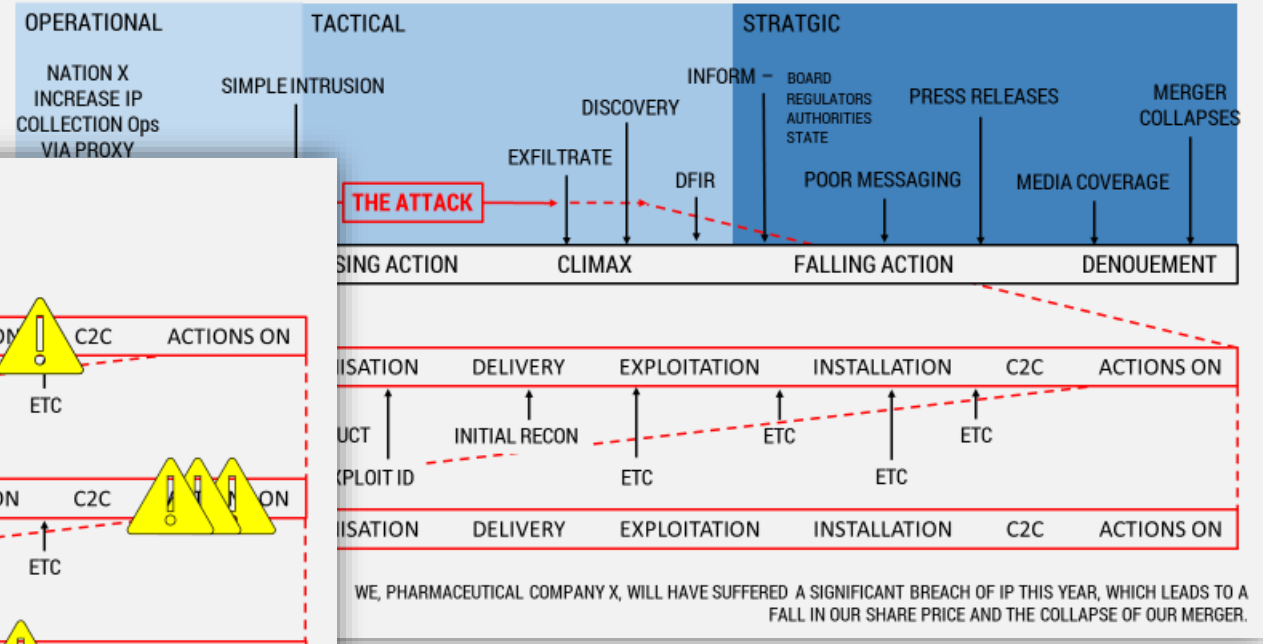
+

CONE OF PLAUSIBILITY - BASELINE

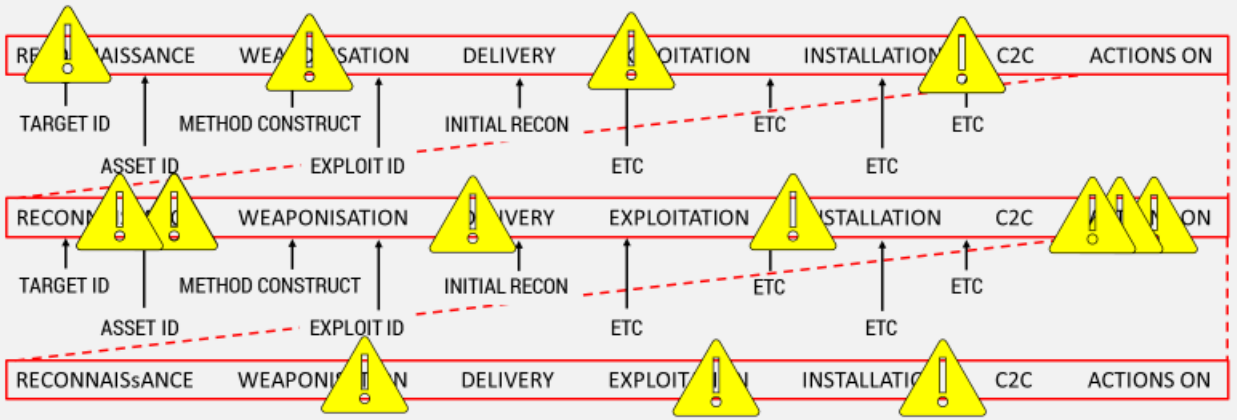
SOCIAL	RELIANCE ON SM – INTERNAL DIVISIONS
TECHNOLOGY	POOR CYBER SECURITY REMAINS
MILITARY	RUSSIA DECREASES SYRIA – INCREASES NATO
POLITICAL	COUNTRY X PLAYS NICELY WITH VLAD
ECONOMIC	REMAINS STAGNANT

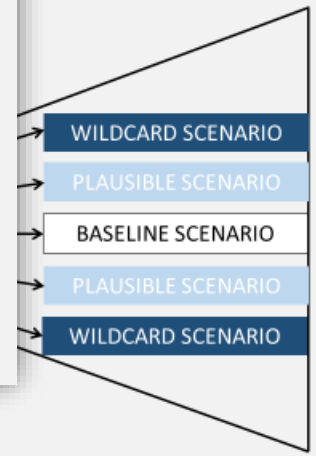
Russia continues to play upon internal political divisions due to economic stagnation & political differences. Poor

BACKCASTING – TIMELINE ANALYSIS



COMBAT INDICATORS (FLAGS AND SIGN POSTS)





PERIOD OF TIME

WHAT ARE WE ULTIMATELY LOOKING TO ACHIEVE?

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

"… IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations."

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

There are four main steps:

- Define the battlefield environment.
- Describe the battlefield’s effects.
- Evaluate the threat.
- Determine threat COAs

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

- Define the battlefield environment.
- Describe the battlefield's effects.
- Evaluate the threat.
- Determine threat COAs

STEMPLES — PESTLE-M

MOTIVES, WEAPONS — CAPABILITY / OPPORTUNITY / INTENT, TTP'S

SO WHAT!!

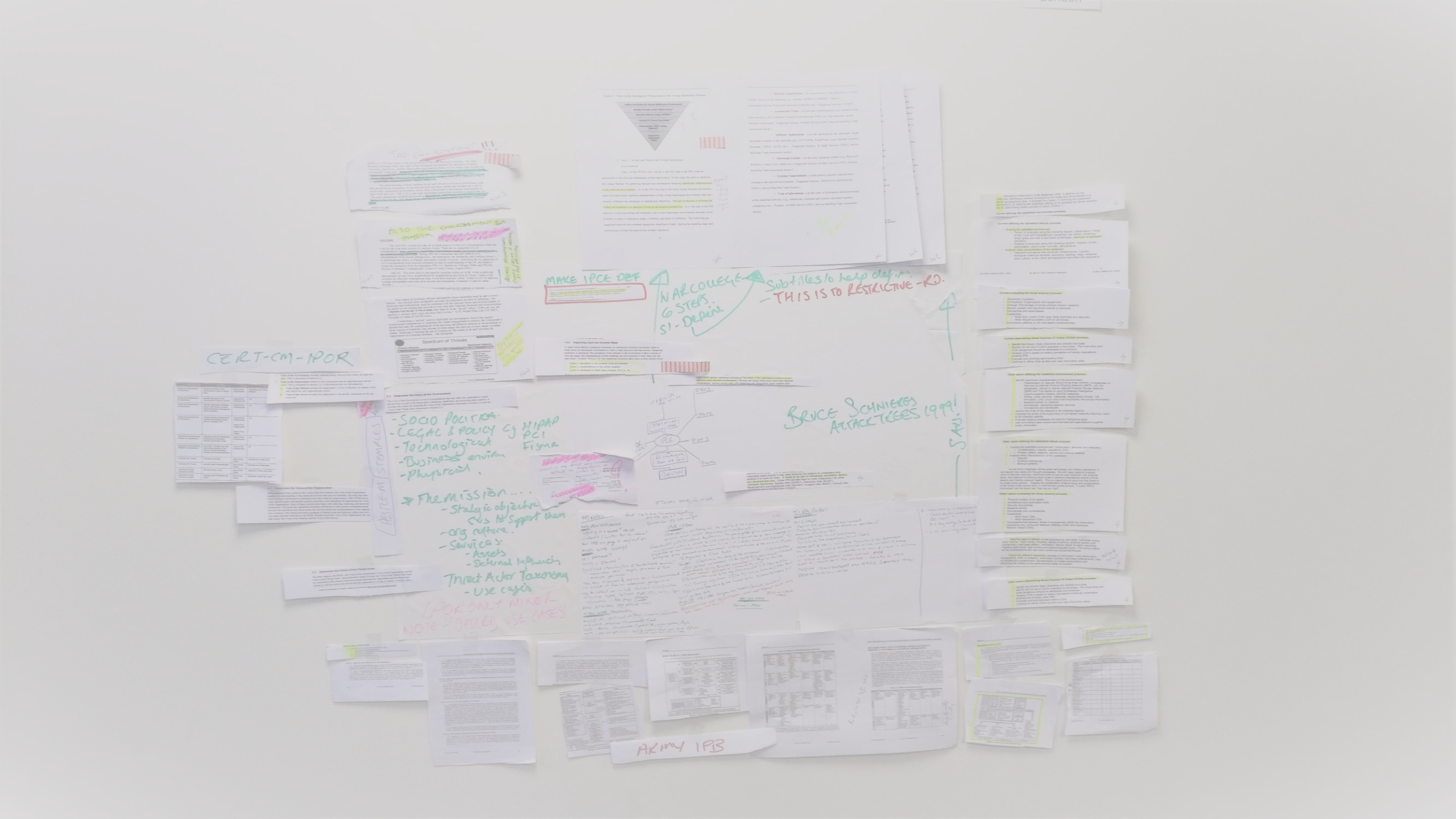
SEQUENCE OF EVENTS

SIG POSTS & FLAGS

WHAT, WHERE, WHEN, HOW

THIRD ORDER EFFECTS

= 360° UNDERSTANDING OF YOU, THE ENEMY + THE ENVIRONMENT


MAKE IPCE DEF
NARCOLLEGE
6 STEPS
S1 - DEFINE
Subtitles to help clarify
- THIS IS TO RESTRICTIVE - RD.
CERT-CM-IPOR
- SOCIO POLITICAL
- LEGAL & POLICY eg HIPAA PCI Fisma
- Technological
- Business environ
- Physical
- The MISSION ....
- Strategic objectives
CVs to support them
- org culture
- Services
- Assets
- External influences
Threat Actor Taxonomy
- Use cases
IPOR ONLY MINOR NOTE TO DISCUSS USE CASES
BRUCE SCHNEIERS ATTACK TREES 1999!
ARMY IPB

DEFINITION

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

“… IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations.”

DEFINITION

~~INTELLIGENCE PREPARATION OF THE BATTLEFIELD~~

~~“… IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations.”~~

DEFINITION

~~INTELLIGENCE PREPARATION OF THE BATTLEFIELD~~

~~"…IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations ."~~

INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT

"…IPCE is a systematic and continuous process of analysing: the means and motives of threat actors; your digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which you will face threats, enhancing your operational resiliency."

DEFINITION

INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT

"…IPCE is a systematic and continuous process of analysing: the means and motives of threat actors; your digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which you will face threats, enhancing your operational resiliency."

SANS
"It (IPB) needs to be part of rehearsals, simulation, testing and development now."

CERT-RMM
"The ability of the organisation to achieve its mission even under degraded circumstances."

Carnegie Mellon University – SEI
"The key to success in defining the virtual environment is to analyse it from an adversarial point of view."

DEFINITION

INTELLIGENCE PREPARATION OF THE CYBER ENVIRONMENT

"…IPCE is a systematic and continuous process of analysing; the means and motives of threat actors; our digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which we will face threats, enhancing your operational resiliency."

SANS
"It (IPB) needs to be part of rehearsals, simulation, testing and development now."

CERT-RMM
"The ability of the organisation to achieve its mission even under degraded circumstances."

Carnegie Mellon University – SEI
"The key to success in defining the virtual environment is to analyse it from an adversarial point of view."

Stages of IPB

	SEI	US Army	SANS
STEP ONE	Determine the voice of the Environment	Define the Operational Environment	Define the Battlefield
STEP TWO	Determine the voice of the organisation	Describe environmental effects on operations	Define the Battlefield effects
STEP THREE	Determine the voice of the Threat Actor	Evaluate the Threat	Evaluate the Threat
STEP FOUR	(3b) Describe use cases	Determine Threat (CoA)	Determine Courses of Actions

4 Stage of IPCE

Determine

In Layman's Terms

Know yourself and your environment, know the bad guys, know what different compromises could look like and understand what could alter or influence all of the above.

FULL SITUATIONAL AWARENESS?

SITUATIONAL AWARENESS

"The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status into the near future."

This Situation awareness takes place at three distinct stages

Level 1:
Perception of the elements in the environment

Level 2:
Comprehension of the current situation

Level 3:
Projection of the future status

- Endsley 2012, p13

“The key to success in analysing the environment is to assess it from the enemy perspective.”

– Naval War college

THERE ARE 3 PERSPECTIVES TO CONSIDER

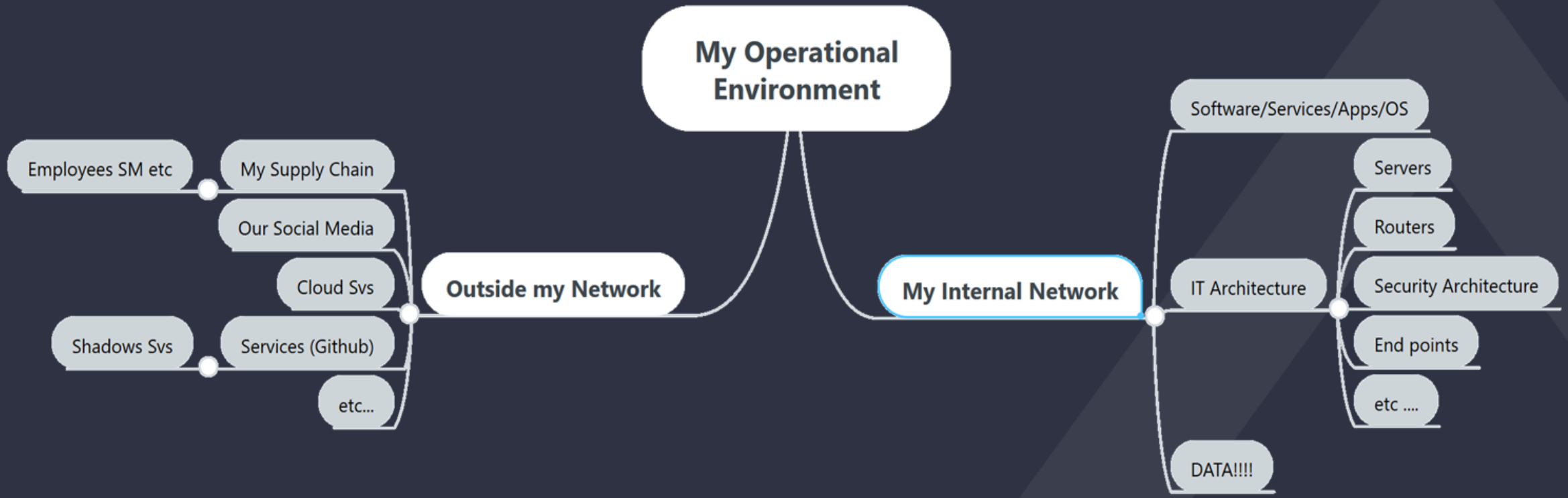
FRIENDLY FORCES

NEUTRAL FORCES

ENEMY FORCES

STEP 1
DETERMINE THE OPERATIONAL ENVIRONMENT

Step 1: Determine the Operational Environment



STEP 2
DETERMINE INFLUENCES ON THE OPERATIONAL ENVIRONMENT

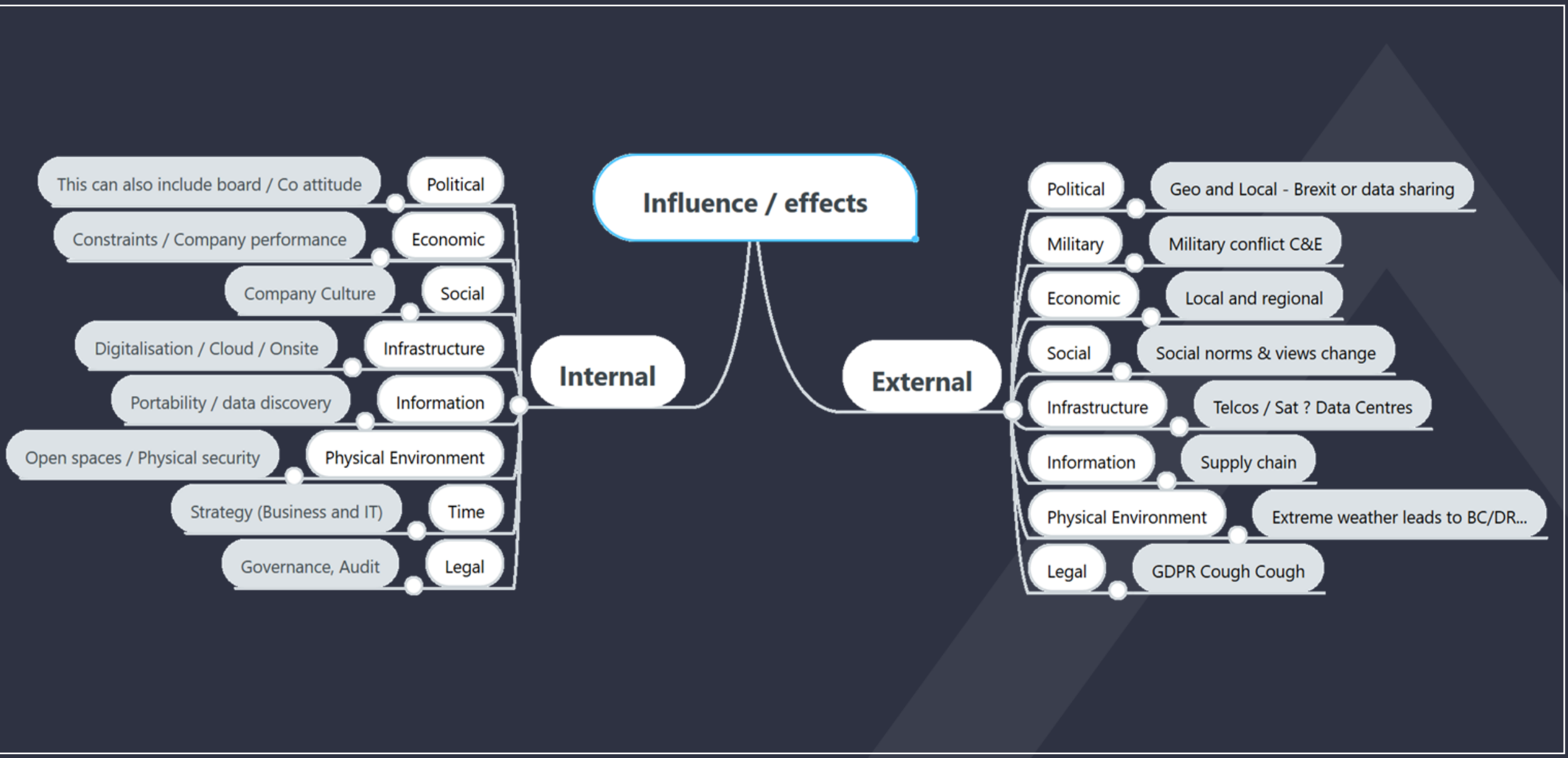
Determine influences on the Environment

- **P** OLITICAL
- **E** CONOMIC
- **S** OCIAL
- **T** ECHNOLOGICAL
- **L** EGAL
- **E** NVIRONMENTAL
- **-**
- **M** ILITARY

- **S** OCIAL ✓
- **T** ECHNOLOGICAL
- **E** CONOMIC
- **M** ILITARY
- **P** OLITICAL
- **L** EGAL ✓
- **E** NVIRONMENTAL

- **P** OLITICAL ✓
- **M** ILITARY ✓
- **E** CONOMIC ✓
- **S** OCIAL ✓
- **I** NFRASTRUCTURE ✓
- **I** NFORMATION ✓
- **-**
- **P** HYS ENVIRONMENT ✓
- **T** IME ✓

Step 2: Determine influences on the Environment



STEP 3:
DETERMINE THE THREAT ACTORS

Step 3: Determine the Threat Actors

Ultimately you want to know;

Who, what, where, when, how and why.

But how do you answer that…

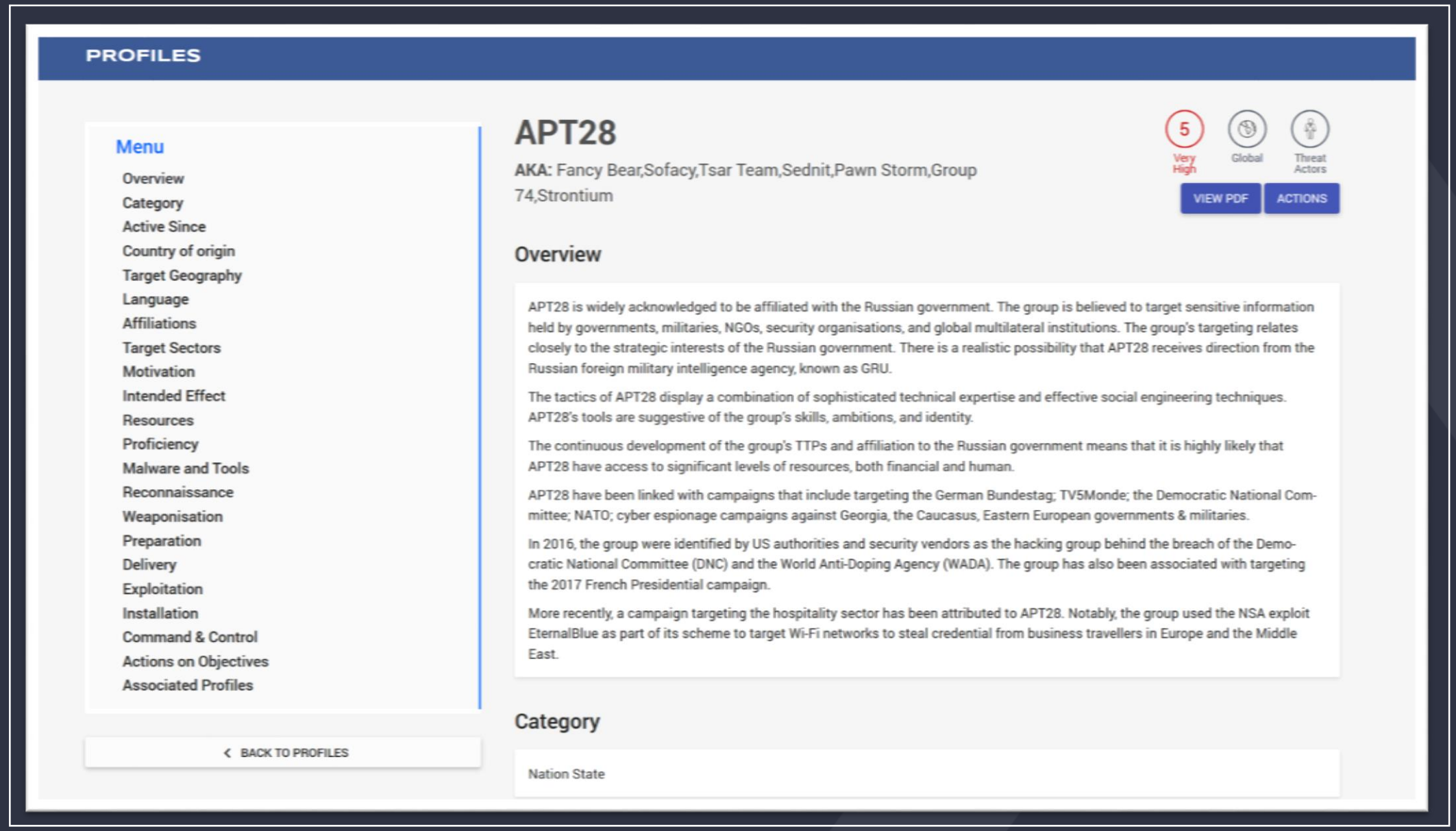
Step 3: Determine the Threat Actors – Start big (even bigger than this?)

	Payment Traffic	Cash Management	Trading Platform	Exchange Traffic
OCG	20	20	20	20
Nation State	15	20	15	20
Insider	20	20	20	15
Hacker	12	15	9	9
Hacktivist	9	9	6	6
Corporations	12	9	12	15
Terrorists	8	8	8	2

Step 3: Determine the Threat Actors – Then get more granular

	Payment Traffic	Cash Management	Trading Platform	Exchange Traffic
OCG Y	20	20	20	20
OCG Y	15	20	15	20
OCG Y	20	20	20	15
APT X	12	15	9	9
APT Proxy X	9	9	6	6
Hacker Z	12	9	12	15
Hacker Z	8	8	8	2

Step 3: Determine the Threat Actors – What to collect



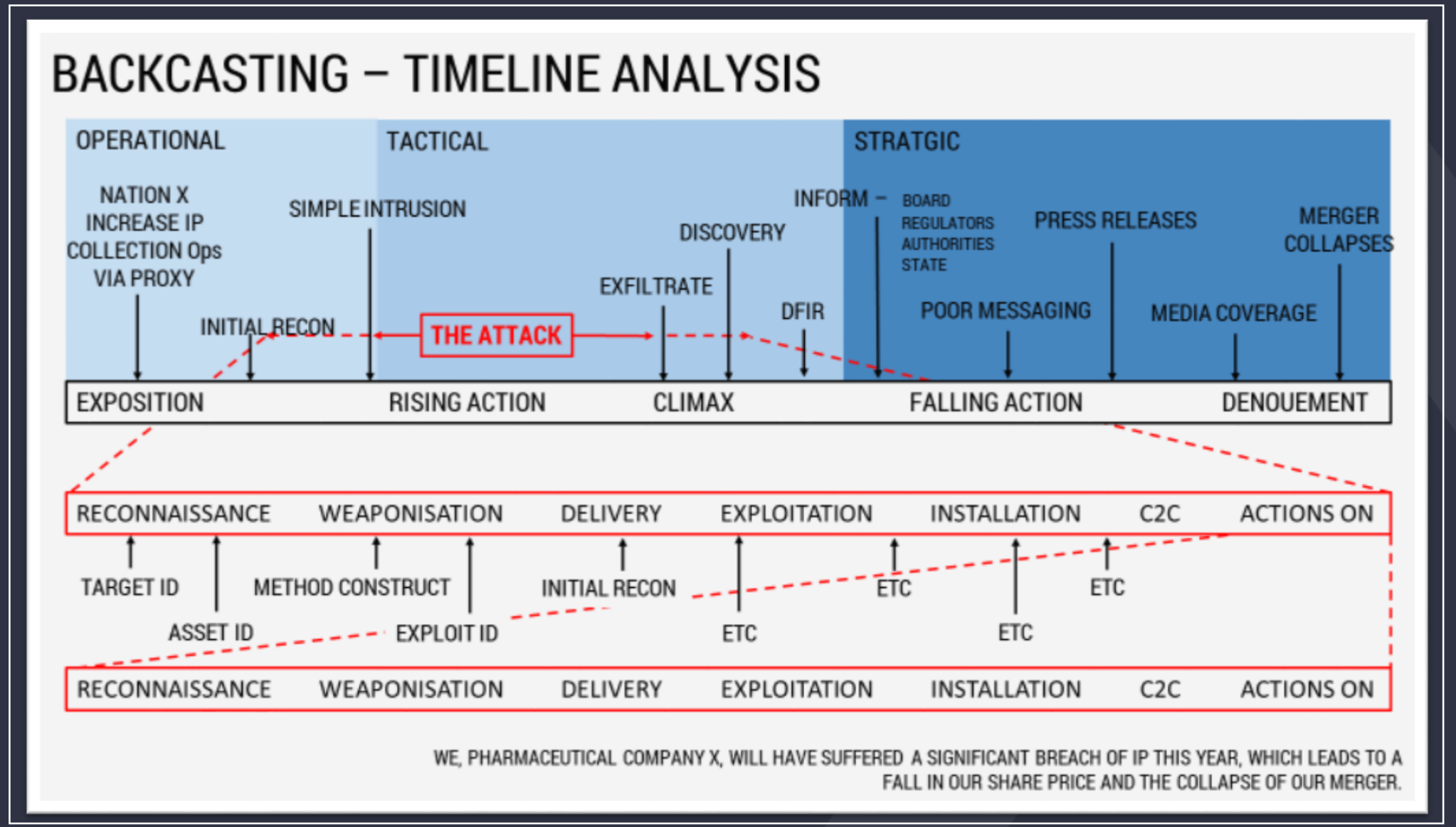
STEP 4
DETERMINE THE THREAT SCENARIOS

Step 4: Determine the Threat Scenarios – MLCoA Vs MDCoA

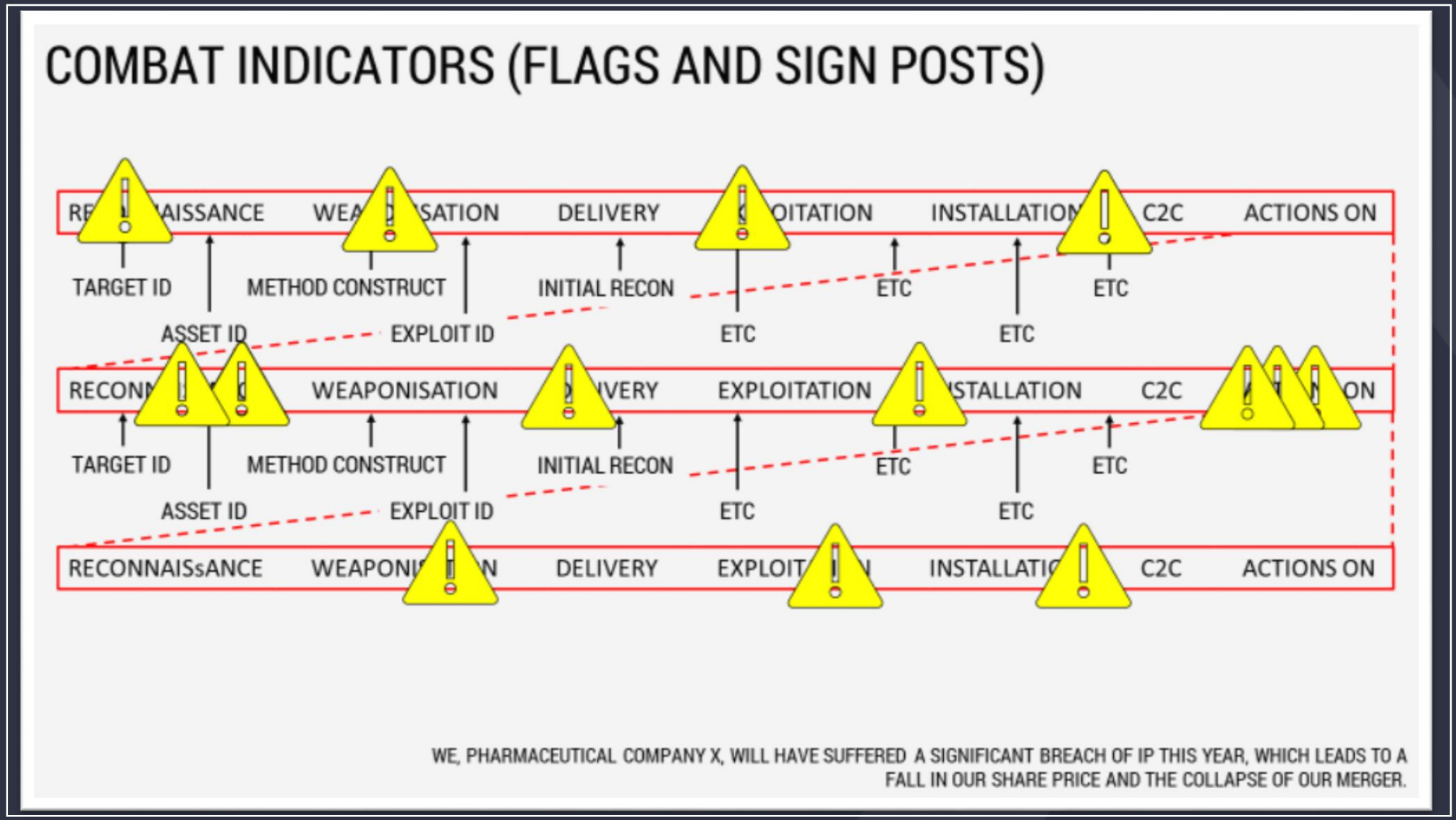
Scenario	Capability	Intent	Threat Score
MLCoA: Scenario 1 – An OCG targets the Cash Management to siphon money from the organisation	4	5	20
MLCoA: Scenario 2 – An OCG manipulates the xxxxxxx to manipulate stock market prices	4	5	20
MLCoA: Scenario 3 – An insider conspires to sell PII and financial information from x asset	4	5	20
MDCoA: Scenario 4 – Lazarus Group compromises the Cash Management assets to perform SWIFT transfers involving large amounts of money	4	4	16

Opportunity and Impact

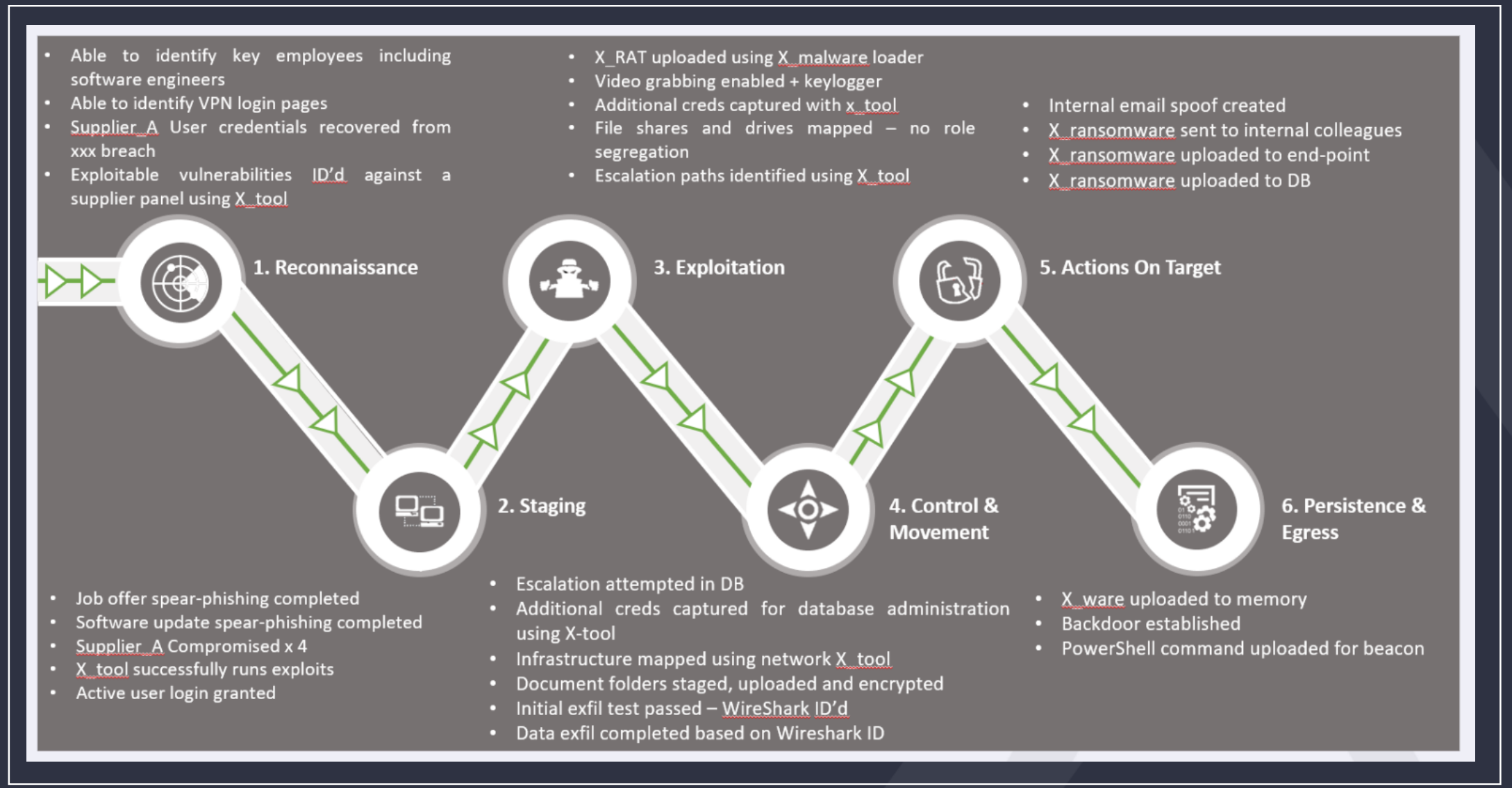
2017


BACKCASTING – TIMELINE ANALYSIS
OPERATIONAL
TACTICAL
STRATGIC
NATION X INCREASE IP COLLECTION Ops VIA PROXY
SIMPLE INTRUSION
DISCOVERY
INFORM – BOARD REGULATORS AUTHORITIES STATE
PRESS RELEASES
MERGER COLLAPSES
EXFILTRATE
DFIR
INITIAL RECON
THE ATTACK
POOR MESSAGING
MEDIA COVERAGE
EXPOSITION
RISING ACTION
CLIMAX
FALLING ACTION
DENOUEMENT
RECONNAISSANCE
WEAPONISATION
DELIVERY
EXPLOITATION
INSTALLATION
C2C
ACTIONS ON
TARGET ID
ASSET ID
METHOD CONSTRUCT
EXPLOIT ID
INITIAL RECON
ETC
ETC
ETC
ETC
RECONNAISSANCE
WEAPONISATION
DELIVERY
EXPLOITATION
INSTALLATION
C2C
ACTIONS ON
WE, PHARMACEUTICAL COMPANY X, WILL HAVE SUFFERED A SIGNIFICANT BREACH OF IP THIS YEAR, WHICH LEADS TO A FALL IN OUR SHARE PRICE AND THE COLLAPSE OF OUR MERGER.

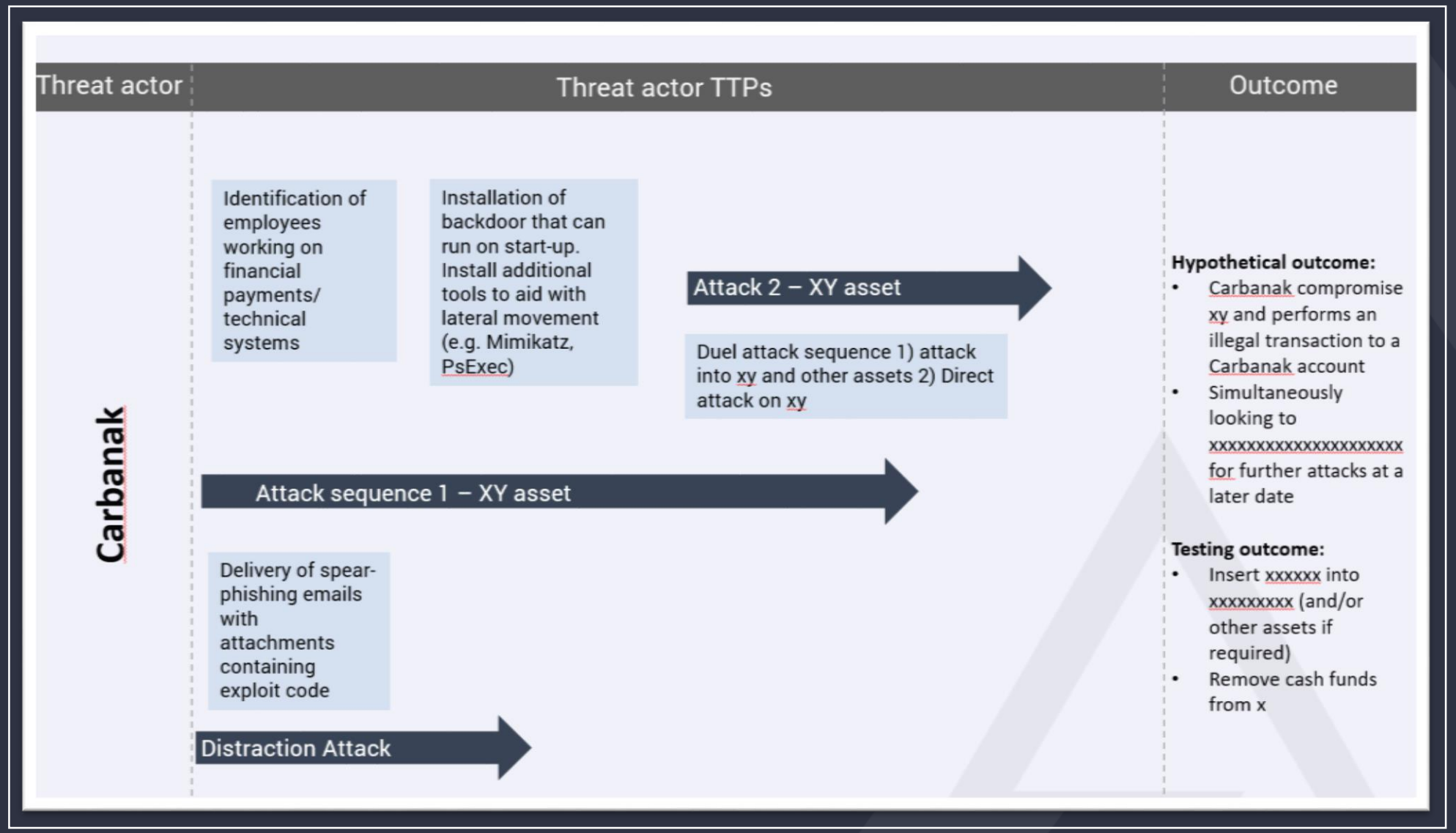
2017


COMBAT INDICATORS (FLAGS AND SIGN POSTS)
TARGET ID
ASSET ID
METHOD CONSTRUCT
EXPLOIT ID
INITIAL RECON
ETC
ETC
ETC
ETC
WEAPONISATION
EXPLOITATION
C2C
TARGET ID
ASSET ID
METHOD CONSTRUCT
EXPLOIT ID
INITIAL RECON
ETC
ETC
ETC
ETC
RECONNAISSANCE
DELIVERY
C2C
ACTIONS ON
WE, PHARMACEUTICAL COMPANY X, WILL HAVE SUFFERED A SIGNIFICANT BREACH OF IP THIS YEAR, WHICH LEADS TO A FALL IN OUR SHARE PRICE AND THE COLLAPSE OF OUR MERGER.

Step 4: Determine the Threat Scenarios – Mapping

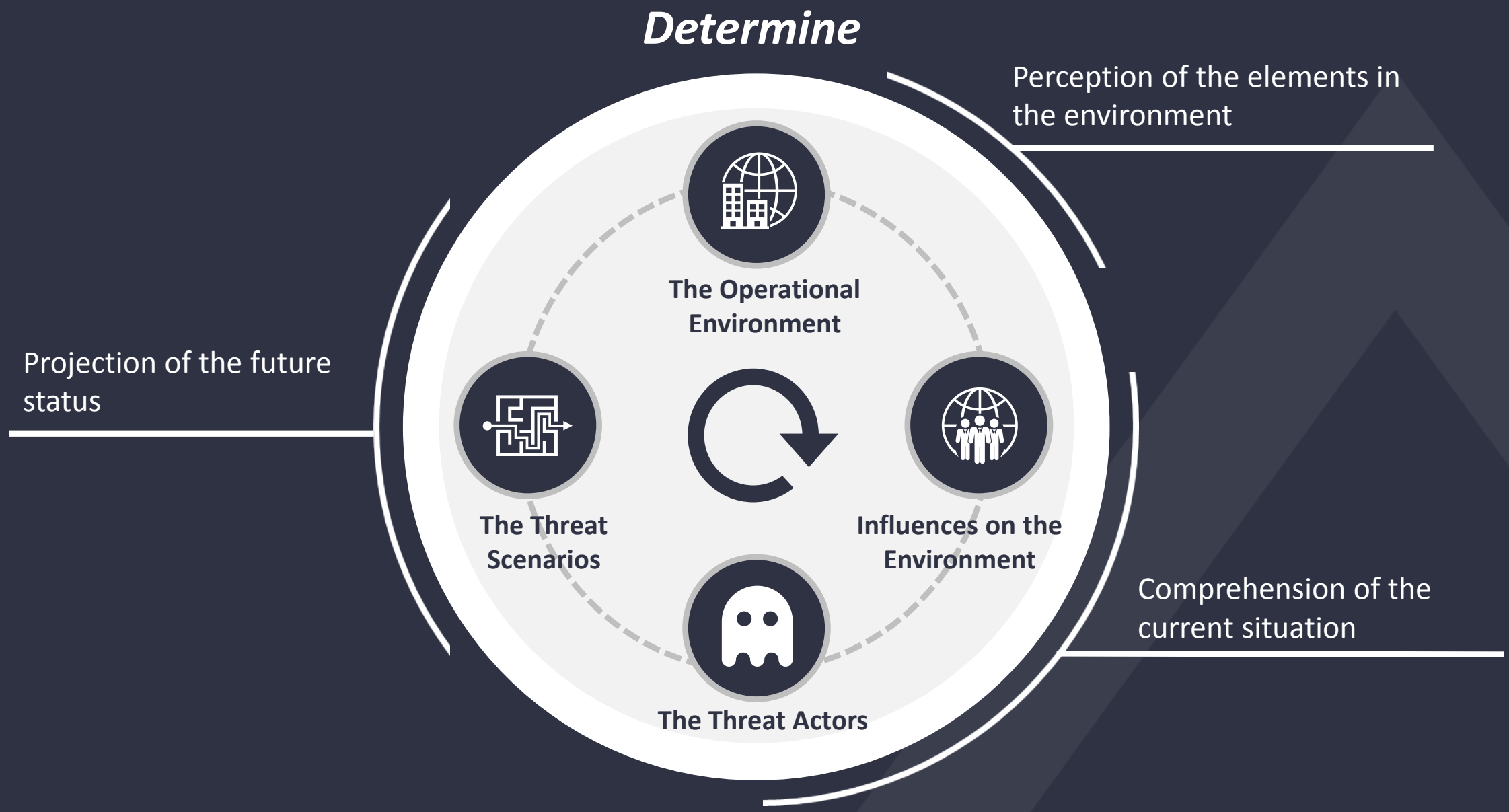


Step 4: Determine the Threat Scenarios - Mapping



So…where are we?

Situational Awareness



Levels of Maturity

Level 1: Perceived

Level 1: Dangerous

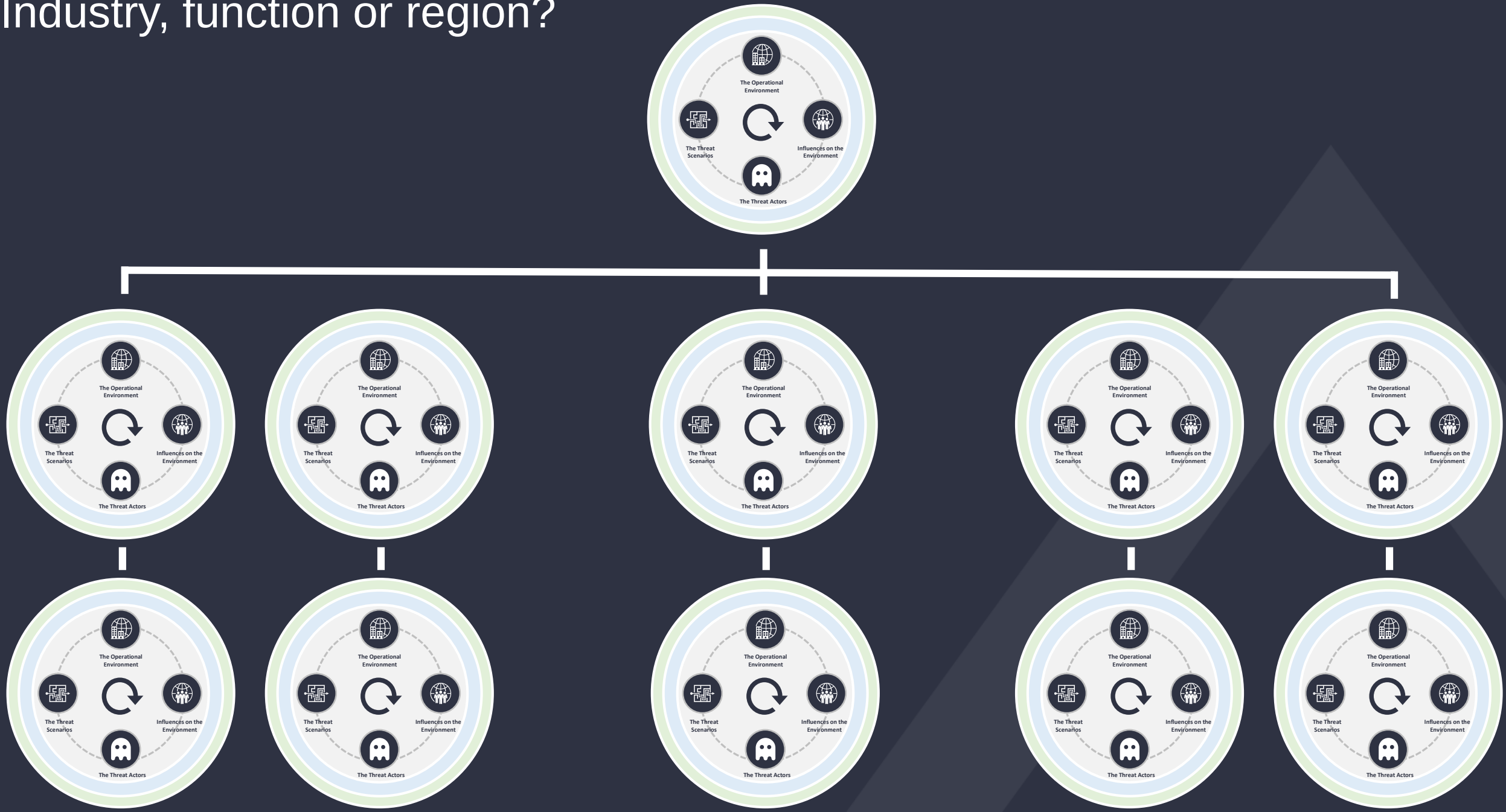
Level 2: Understood

Level 2: Baseline

Level 3: Horizon Scan

Level 3: Aspirational

Industry, function or region?



WHATS NEXT….

SANS Says it Best

"It needs to be part of rehearsals , simulation, testing and development now."

- Simulation Testing
- Blue Team Dev
- Use Case Dev
- DFIR Dev
- Policy Dev
- Strategy & Road Map Dev
- **ICP Dev**

QUESTIONS

With thanks to:

SANS: Use Offense to inform defence. Find the flaws before the bad guys do.
Carnegie Mellon University Software Engineering Institute: Intelligence Preparation for Operational Resilience
US Army and US Marine Corps: Intelligence Preparation of the Battlefield APT2-01.3 / MCRP 2-3A

INTELLIGENCE METHODS

YOUTUBE

SORRY, WHO ARE YOU AGAIN?

ROB DARTNALL

COMPANY TWITTER

@CYBERFUSIONTEAM