

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

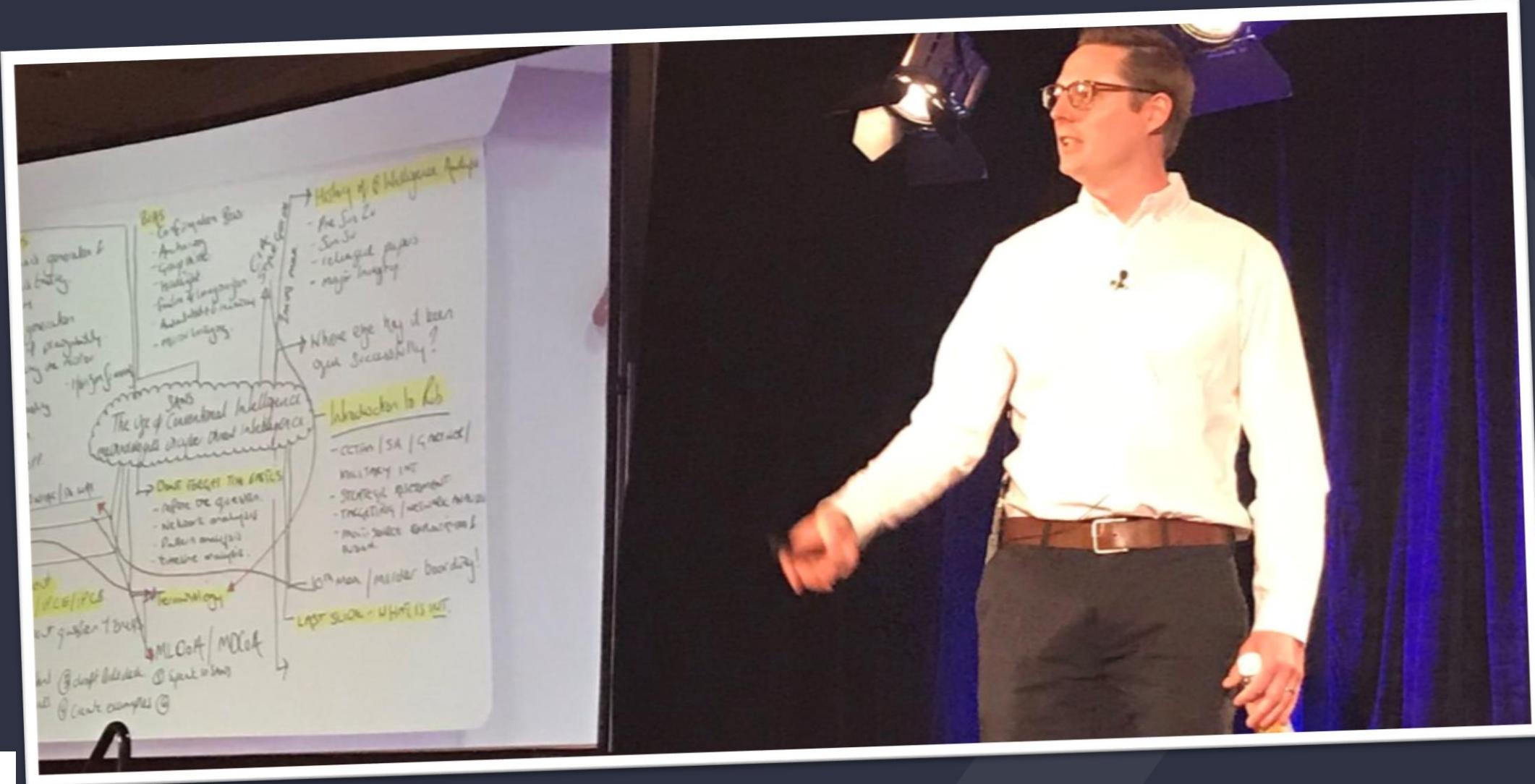
Director – Cyber Intelligence

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.

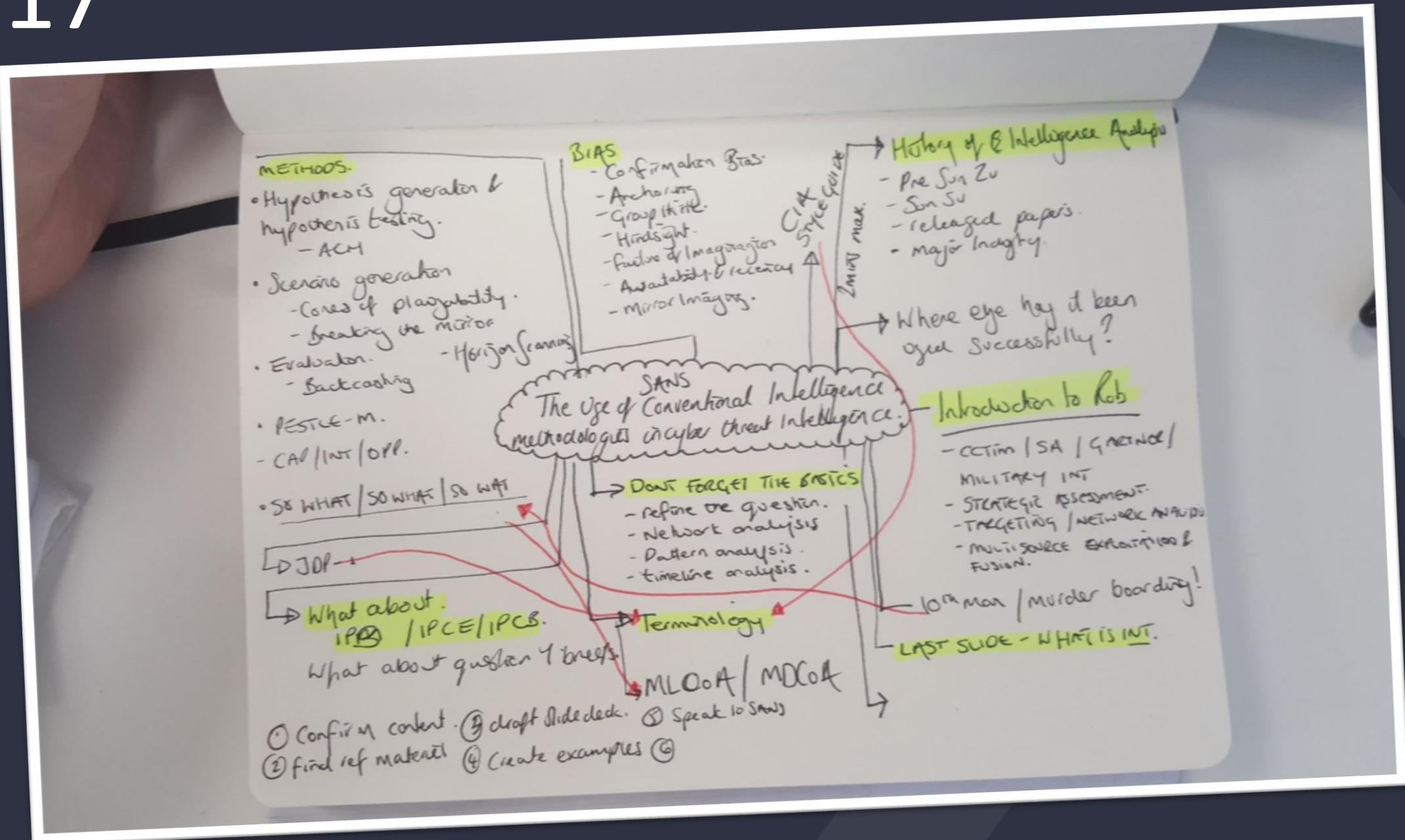
From a conventional Military Intelligence background Mr Dartnall has been **creating cyber threat assessments and building intelligence teams** and testing programs for some of the largest organisations in Europe, North America, the Middle East and Africa.



2017



2017



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

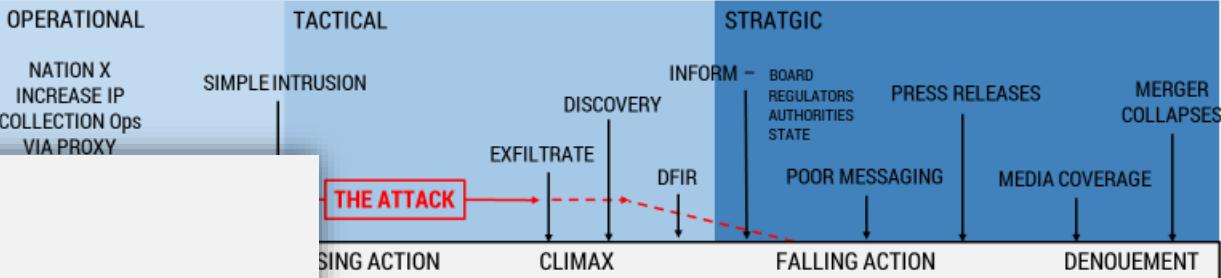


CONE OF PLAUSIBILITY - BASELINE

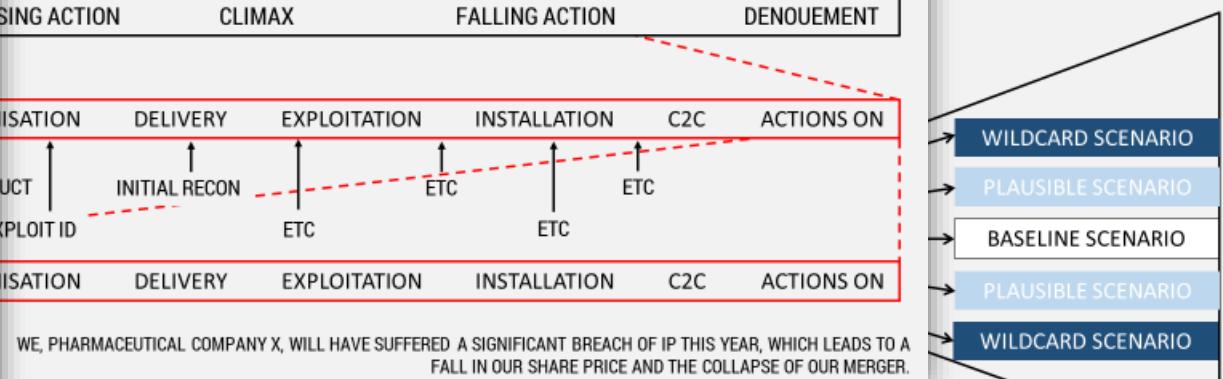
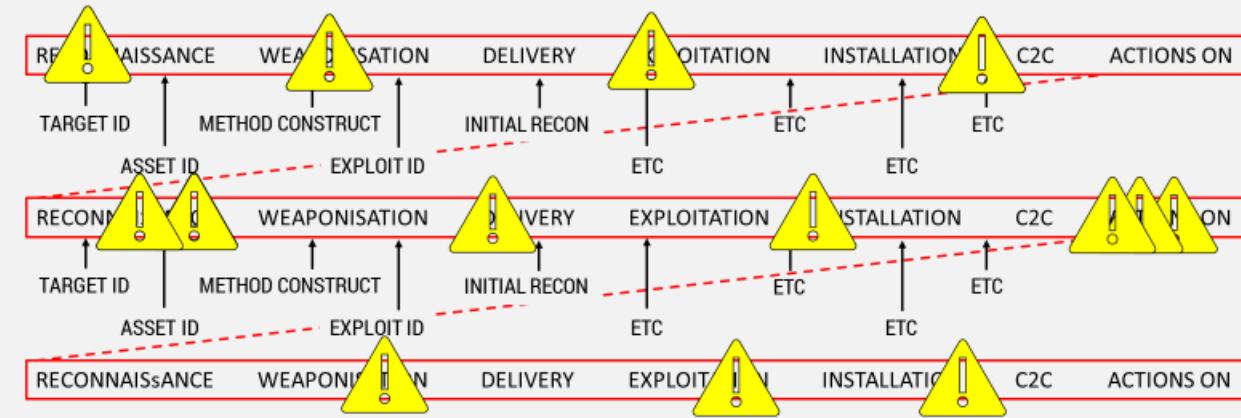
SOCIAL	RELIANCE ON SM – INTERNAL DIVISIONS
TECHNOLOGY	POOR CYBER SECURITY REMAINS
MILITARY	RUSSIA DECREASES SYRIA – INCREASES NATO
POLITICAL	COUNTRY X PLAYS NICELY WITH VLAD
ECONOMIC	REMAINS STAGNANT

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

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.

MURDER BOARD

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

WHAT ARE WE ULTIMATELY LOOKING TO ACHIEVE?

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

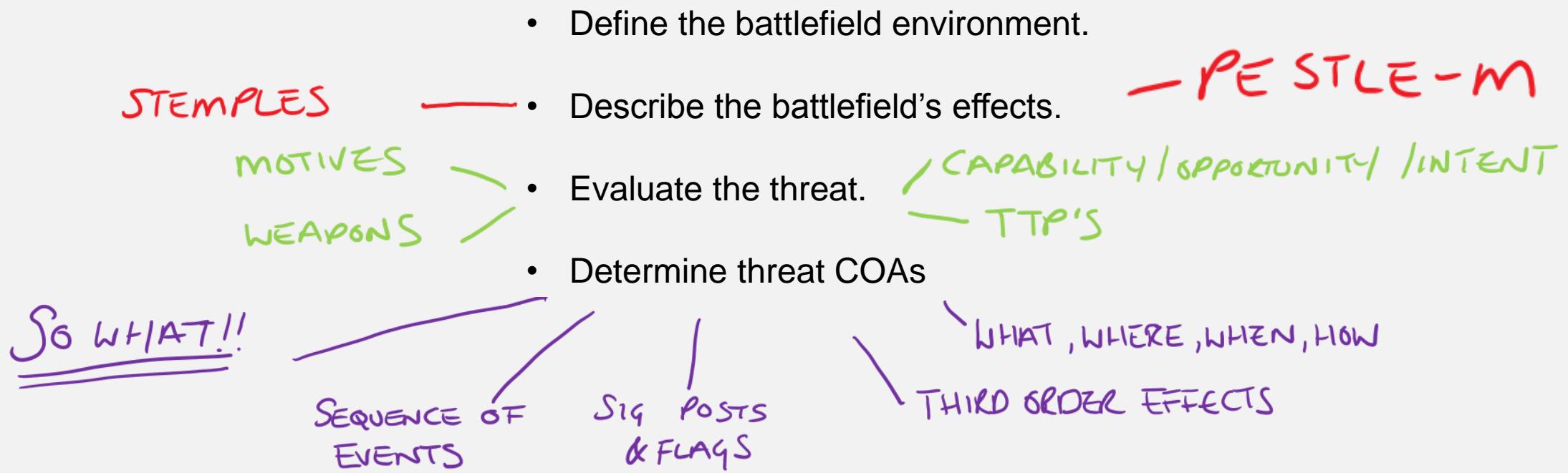
“... IPB is a systematic process of analysing the mission variables of the enemy, terrain, weather and civil considerations in an area of interest to determine their effect on operations.”

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

There are four main steps:

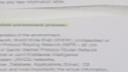
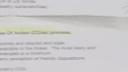
- Define the battlefield environment.
- Describe the battlefield's effects.
- Evaluate the threat.
- Determine threat COAs

INTELLIGENCE PREPARATION OF THE BATTLEFIELD



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

CERT-CM-1P0R



DEFINITION

The Business Club

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

It is believed that the **Dridex** threat group began their operations in 2009 using the **Zeus** malware until 2014. It is widely believed that former Soviet Bloc territories lie “the well-known cybercriminal capability.”

“...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.”

THREAT CHARACTERISTIC

Threat Severity

Active Since

Source

Russia, Worldwide

TARGET SECTOR	TARGET AREAS	RESOURCES	SKILLS	MOTIVATION	ATTACK	CAPABILITY
Finance/Banking	Personnel, network, systems	Well financed, access to high level cybercrime services and resources	Complex malware development and deployment, well executed attacks	Financial gain	Mainly in the middle capabilities of Dridex enable personal and financial information to be stolen	High



TPPs
Plan
Epidemic of malicious software infections, such as viruses, worms, Trojans, or spyware, can spread rapidly through computer networks and the Internet, causing significant damage to individual computers and entire organizations. These infections can result in the loss of sensitive data, system crashes, and even complete system failures. They can also be used to steal sensitive information, such as financial data, trade secrets, and personal information. In some cases, they can be used to disrupt critical infrastructure, such as power grids, water supply systems, and transportation networks.

Rebates. Documents contain obfuscated macros which download the payload

- Communication with C2 server is often heavily encrypted with XOR cipher

DEFINITION

The Business Club

INTELLIGENCE PREPARATION OF THE BATTLEFIELD

It is believed that the Russian government began developing its IPB operations in 2009 using the Stuxnet worm as a template. It was not until 2014 that it was widely believed that former Soviet Bloc territories led “the world in” developing their own cybercriminal capability.

“...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.”



THREAT CHARACTERISTIC

Threat Severity

Active Since

Source

TARGET SECTOR	TARGET AREAS	RESOURCES	SKILLS	MOTIVATION	ATTACK	CAPABILITY
Finance/Banking	Personnel, network, systems	Well financed, access to high level cybercrime services and resources	Complex malware development and deployment, well executed attacks	Financial gain	Mainly in the middle capabilities of Dridex enable personal and financial information to be stolen	High

DEFINITION

The Business Club



INTELLIGENCE PREPARATION OF THE BATTLEFIELD

It is believed that the Business Club carried out operations in 2009 using the Gameover Zeus malware until 2014. It is also believed that former SCADA system operators lead the cyber campaign.

“...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 .”

THREAT CHARACTERISTIC

Threat Severity

Active Since

Source

TARGET SECTOR

TARGET AREAS

Finance/Banking

Personnel,
network,
systems

TPPs

2009

- Emails containing malicious files often pose as invoices, or notifications of tax rebates. Documents contain obfuscated macros which download the payload
- Once executed, the Dridex malware downloads a set of C2 OP addresses

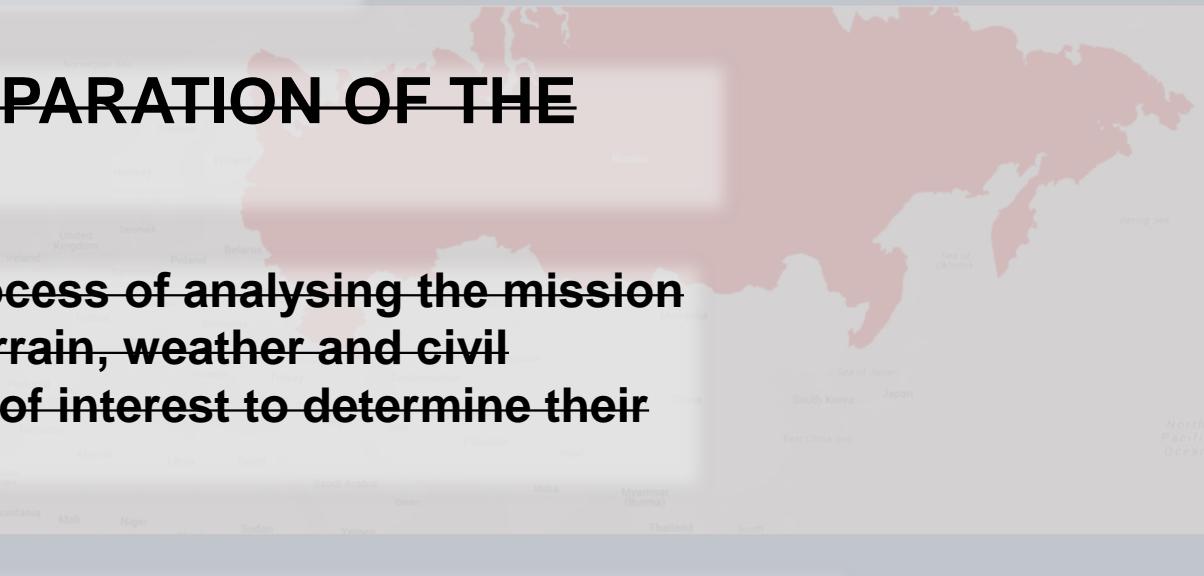
“...IPCE is a systematic and continuous process of analysing: the means and motives of threat actors; your digital environment and the digital environment in which you operate; in order to understand the likely scenarios in which you will face threats, enhancing your operational resiliency.”

Complex malware development and deployment, well executed attacks

Financial gain

Mainly in the middle capabilities of Dridex enable personal and financial information to be stolen

High



DEFINITION

The Business Club



It is believed that the Business Club began their operations in 2009 using the

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.”

THREAT CHARACTERISTIC

Threat Severity

High

Active Since

2009

Source

SANS

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

TARGET

Financial/Banking

Network/

systems

RESOURCES

Well financed, access to high level cyber services and resources

CERT-RMM

“The ability of the organisation to achieve its mission even under degraded circumstances.”

PERSONNEL

IT STAFF

MANAGERS

FINANCIAL

SECURITY

OPERATIONS

LOGISTICS

ADMINISTRATIVE

OTHER

DATA

INFRASTRUCTURE

MANUFACTURING

TRANSPORTATION

POWER

WATER

FOOD

ANIMALS

ENVIRONMENT

TECHNOLOGY

ARTIFICIAL

INTELLIGENCE

DEFENSE

GOVERNMENT

INDUSTRY

COMMERCE

RELIGION

CULTURE

ART

SCIENCE

MUSIC

ENTERTAINMENT

SPORTS

EDUCATION

RESEARCH

TECHNOLOGY

SCIENCE

MUSIC

ENTERTAINMENT

SPORTS

EDUCATION

RESEARCH

DEFINITION

The Business Club

It is believed that the Business Club began their operations in 2009 using the

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.”

THREAT CHARACTERISTIC

Threat Severity

Active Since

Source

SANS

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

RESOURCES

Well financed, access to high level cyber services and resources

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.”



THREAT CHARACTERISTIC

Threat Severity

Active Since

Source

SANS

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

RESOURCES

Well financed, access to high level cyber services and resources

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



FULL SITUATIONAL AWARENESS?

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.

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



“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

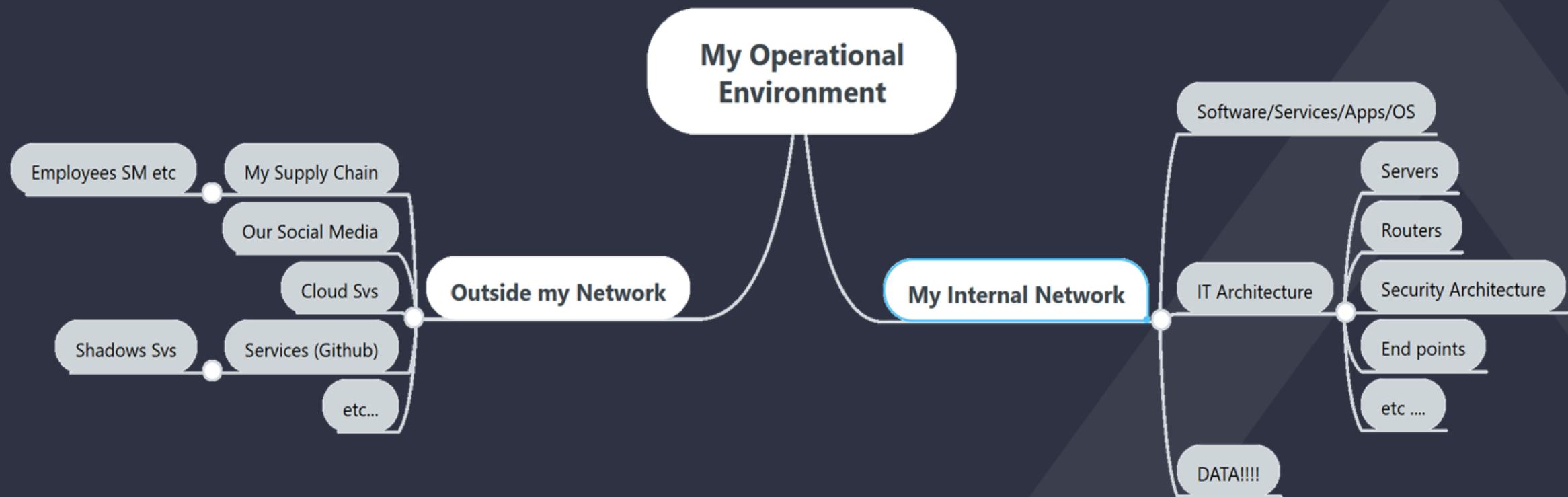


ENEMY
FORCES

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

POLITICAL

ECONOMIC

SOCIAL

TECHNOLOGICAL

LEGAL

ENVIRONMENTAL

MILITARY

SOCIAL ✓

TECHNOLOGICAL

ECONOMIC

MILITARY

POLITICAL

LEGAL ✓

ENVIRONMENTAL

POLITICAL ✓

MILITARY ✓

ECONOMIC ✓

SOCIAL ✓

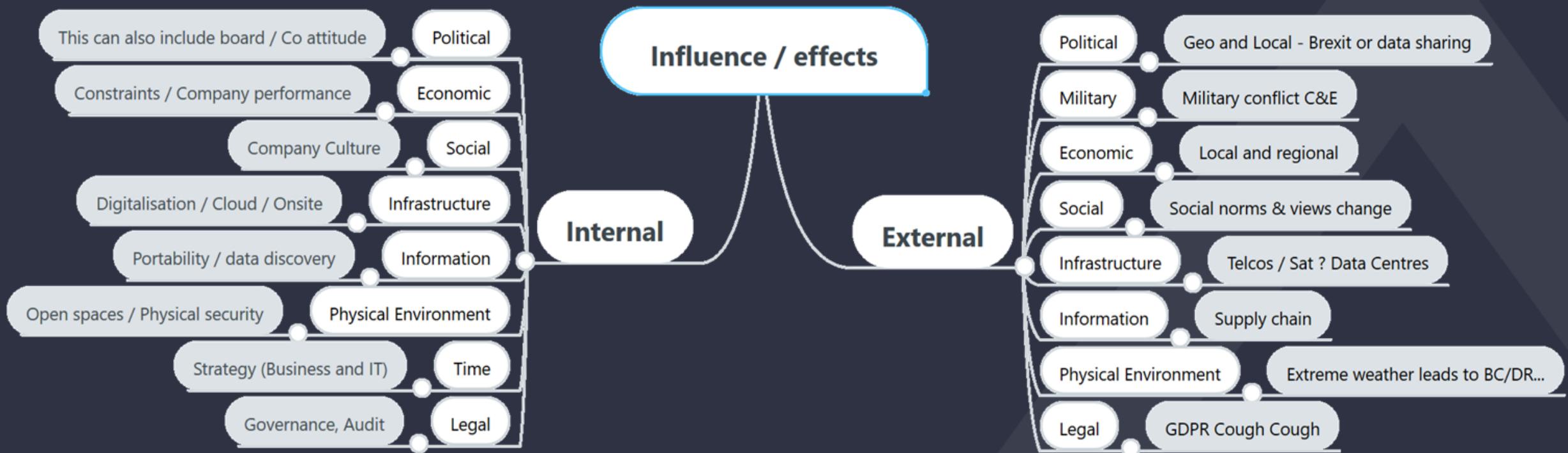
INFRASTRUCTURE ✓

INFORMATION ✓

HYS ENVIRONMENT ✓

IMI ✓

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

PROFILES

Menu

- Overview
- Category
- Active Since
- Country of origin
- Target Geography
- Language
- Affiliations
- Target Sectors
- Motivation
- Intended Effect
- Resources
- Proficiency
- Malware and Tools
- Reconnaissance
- Weaponisation
- Preparation
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives
- Associated Profiles

[**< BACK TO PROFILES**](#)

APT28

AKA: Fancy Bear,Sofacy,Tsar Team,Sednit,Pawn Storm,Group 74,Strontium

5Very High

Global

Threat Actors

[VIEW PDF](#) [ACTIONS](#)

Overview

APT28 is widely acknowledged to be affiliated with the Russian government. The group is believed to target sensitive information held by governments, militaries, NGOs, security organisations, and global multilateral institutions. The group's targeting relates closely to the strategic interests of the Russian government. There is a realistic possibility that APT28 receives direction from the Russian foreign military intelligence agency, known as GRU.

The tactics of APT28 display a combination of sophisticated technical expertise and effective social engineering techniques. APT28's tools are suggestive of the group's skills, ambitions, and identity.

The continuous development of the group's TTPs and affiliation to the Russian government means that it is highly likely that APT28 have access to significant levels of resources, both financial and human.

APT28 have been linked with campaigns that include targeting the German Bundestag; TV5Monde; the Democratic National Committee; NATO; cyber espionage campaigns against Georgia, the Caucasus, Eastern European governments & militaries.

In 2016, the group were identified by US authorities and security vendors as the hacking group behind the breach of the Democratic National Committee (DNC) and the World Anti-Doping Agency (WADA). The group has also been associated with targeting the 2017 French Presidential campaign.

More recently, a campaign targeting the hospitality sector has been attributed to APT28. Notably, the group used the NSA exploit EternalBlue as part of its scheme to target Wi-Fi networks to steal credential from business travellers in Europe and the Middle East.

Category

Nation State

STEP 4

DETERMINE THE THREAT SCENARIOS

Step 4: Determine the Threat Scenarios – MLCoA Vs MDCoA

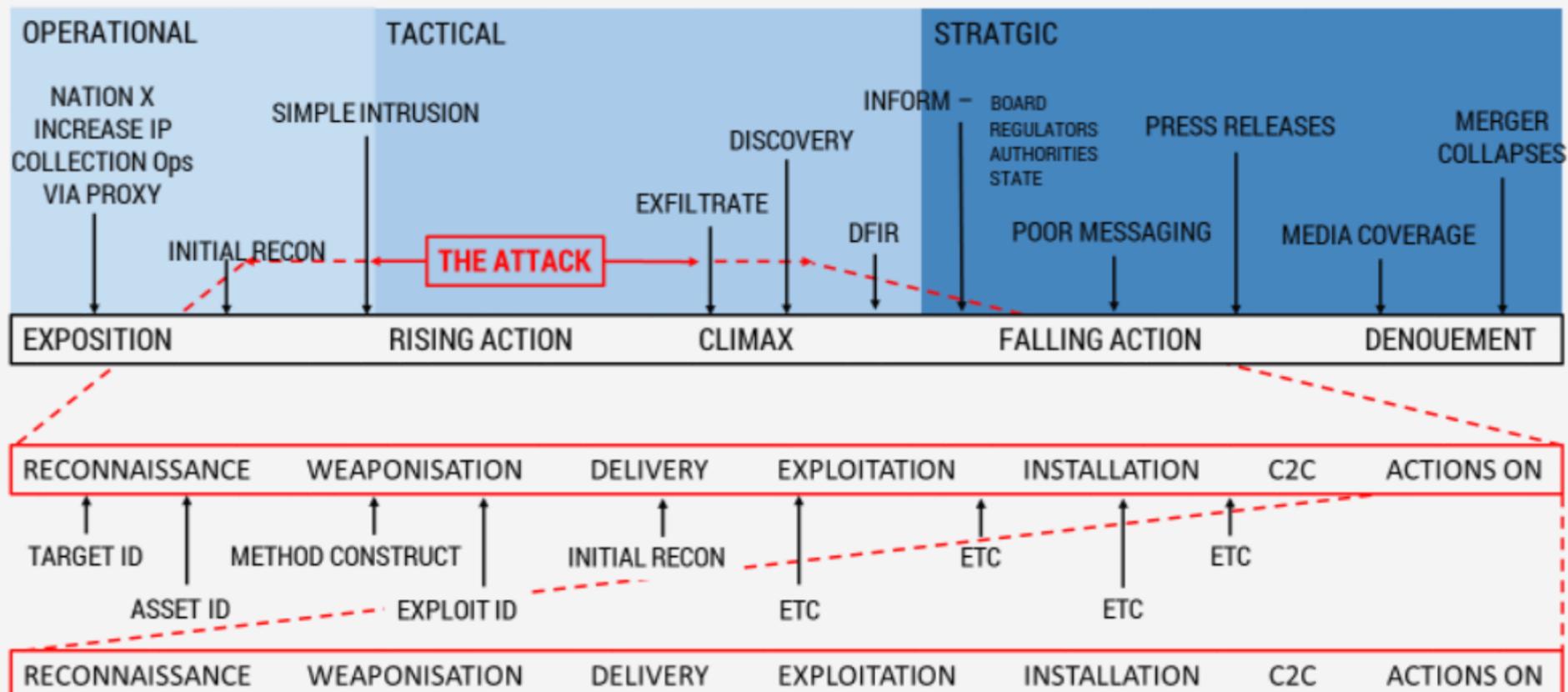
Scenario	Capability	Intent	Threat Score
MLCoA: Scenario 1 – An OCG targets the Cash Management to siphon money from the organisation	4	5	20
MLCoA: Scenario 2 – An OCG manipulates the xxxxxxxx to manipulate stock market prices	4	5	20
MLCoA: Scenario 3 – An insider conspires to sell PII and financial information 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

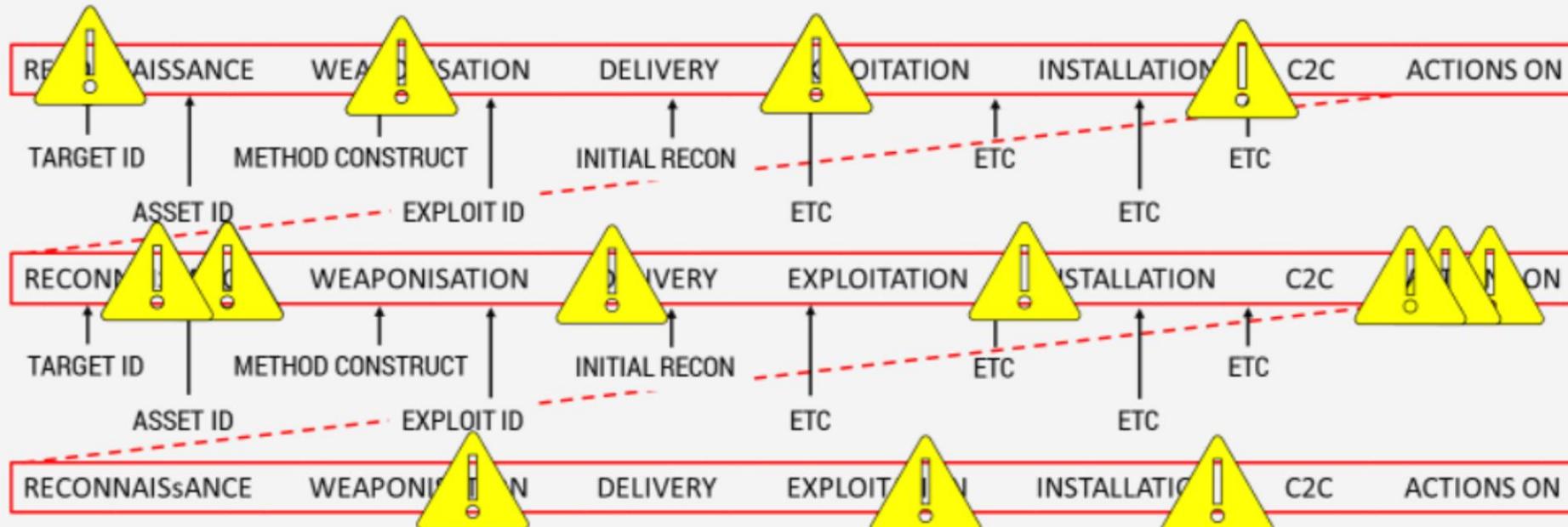
BACKCASTING – TIMELINE ANALYSIS



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.

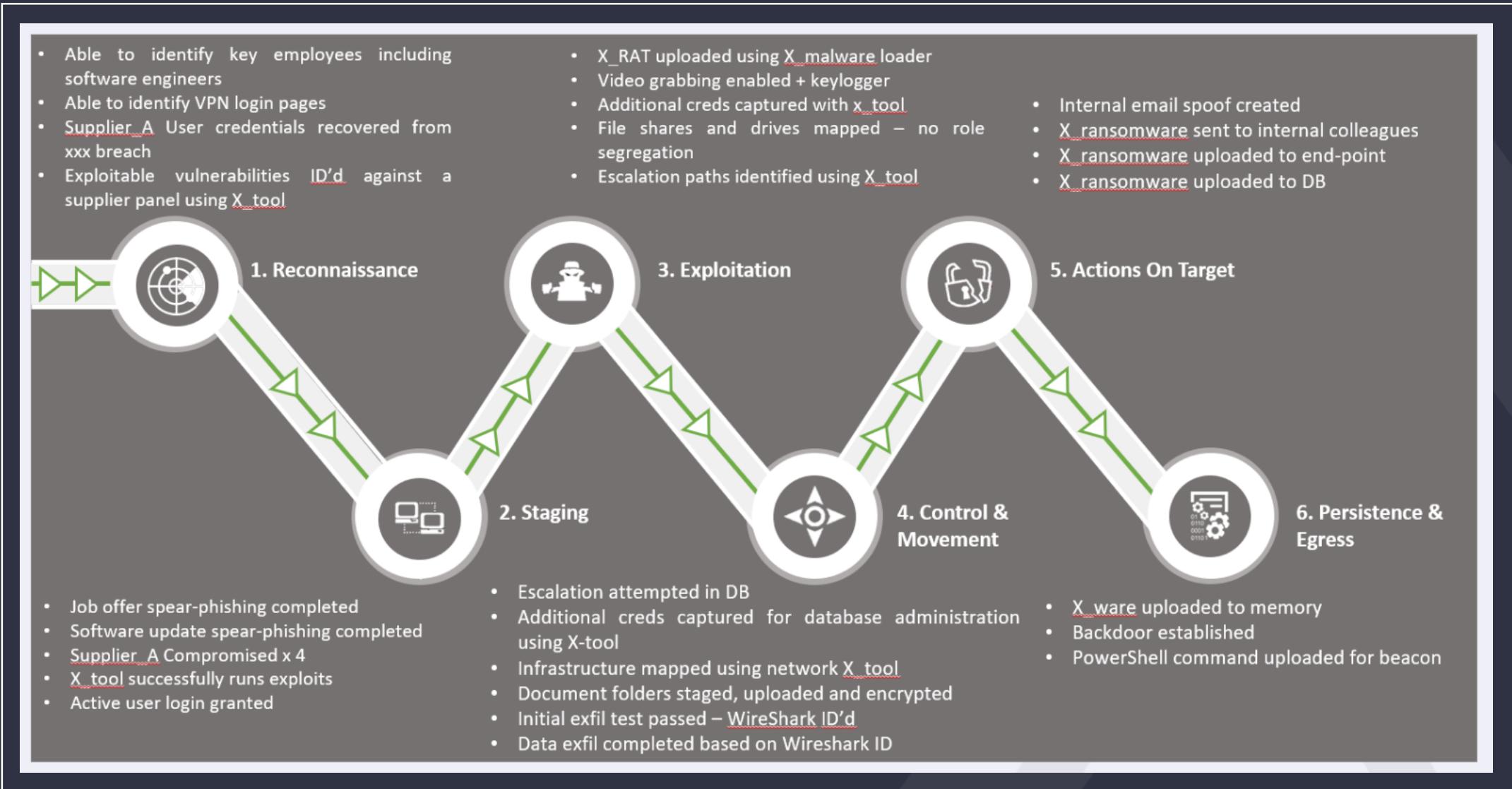
2017

COMBAT INDICATORS (FLAGS AND SIGN POSTS)

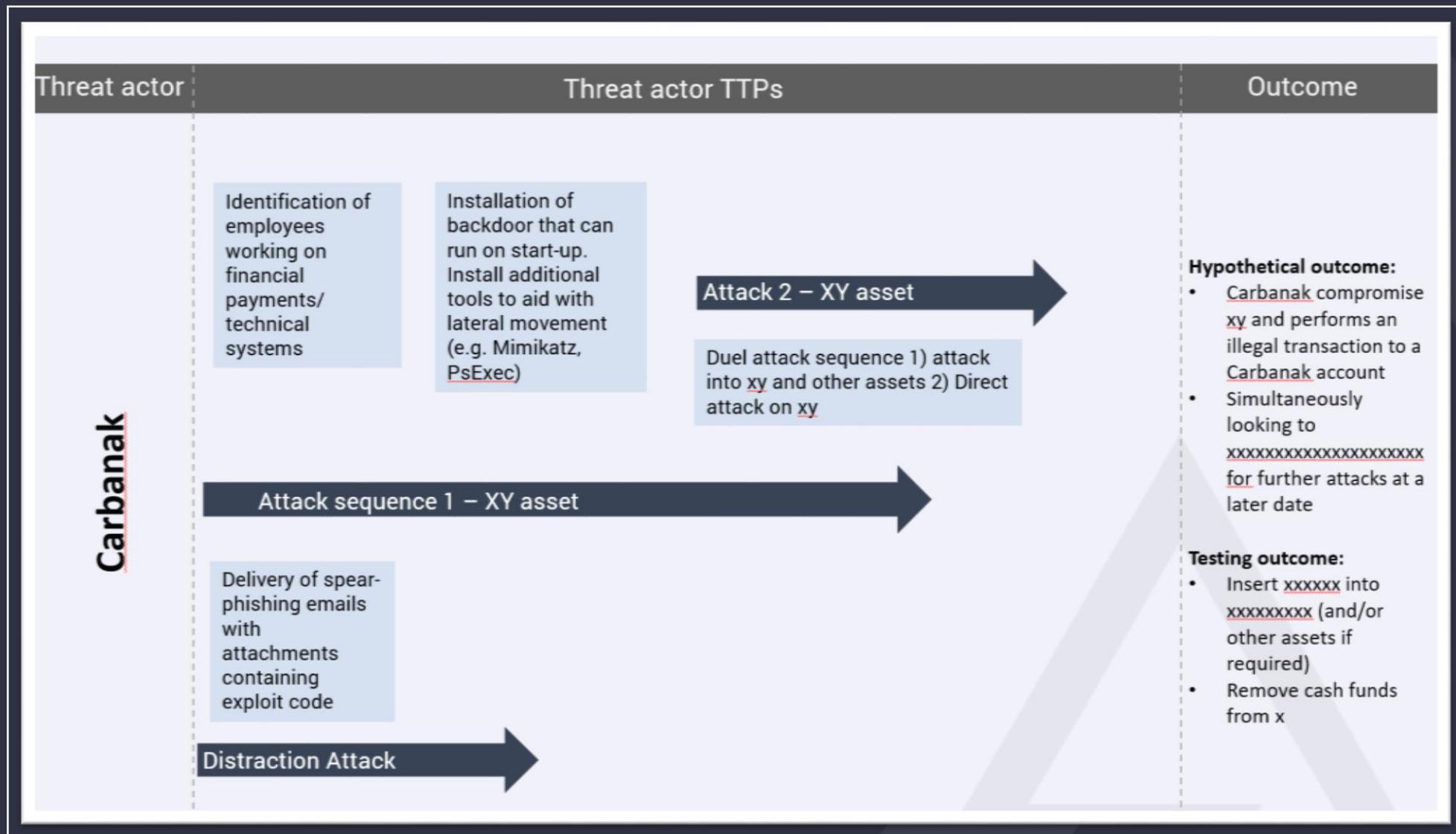


WE, PHARMACEUTICAL COMPANY X, WILL HAVE SUFFERED A SIGNIFICANT BREACH OF IP THIS YEAR, WHICH LEADS TO A FALL IN OUR SHARE PRICE AND THE COLLAPSE OF OUR MERGER.

Step 4: Determine the Threat Scenarios – Mapping

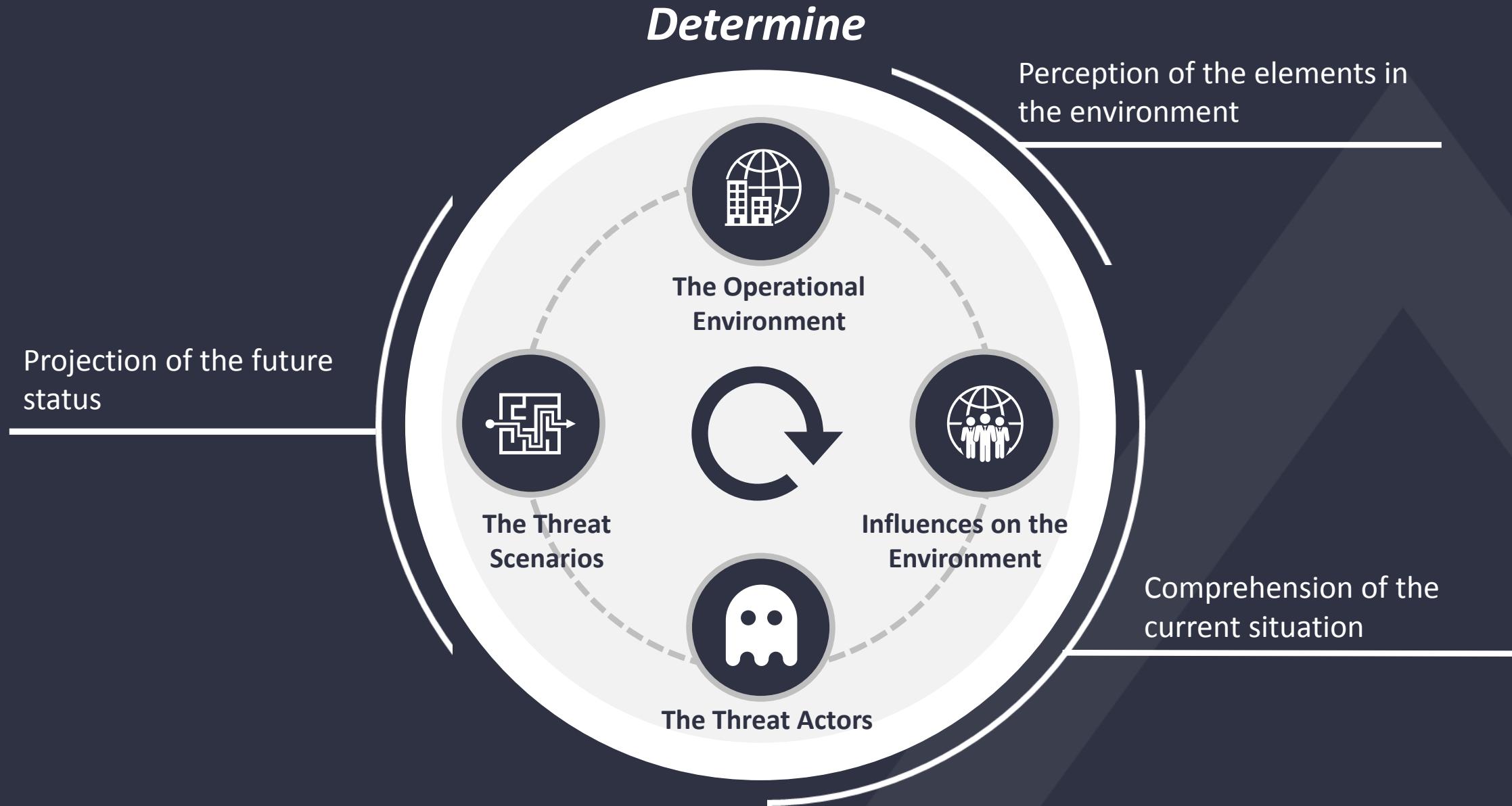


Step 4: Determine the Threat Scenarios - Mapping



So...where are we?

Situational Awareness



Levels of Maturity



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

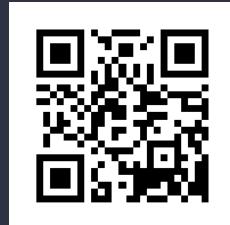
US Army and US Marine Corps: Intelligence Preparation of the Battlefield APT2-01.3 / MCRP 2-
3A

INTELLIGENCE
METHODS



YOUTUBE

SORRY, WHO ARE
YOU AGAIN?



ROB DARTNALL

COMPANY
TWITTER



@CYBERFUSIONTEAM