THE "SMALL" THINGS THAT CTI CAN'T HELP YOU WITH

MAYDAY CONFERENCE, 2019

_ABOUT ME

_Cristi Calita

Cyber Threat Intelligence Consultant

Former Information Risk Analyst @banking

GCTI, OSCP, SSCP

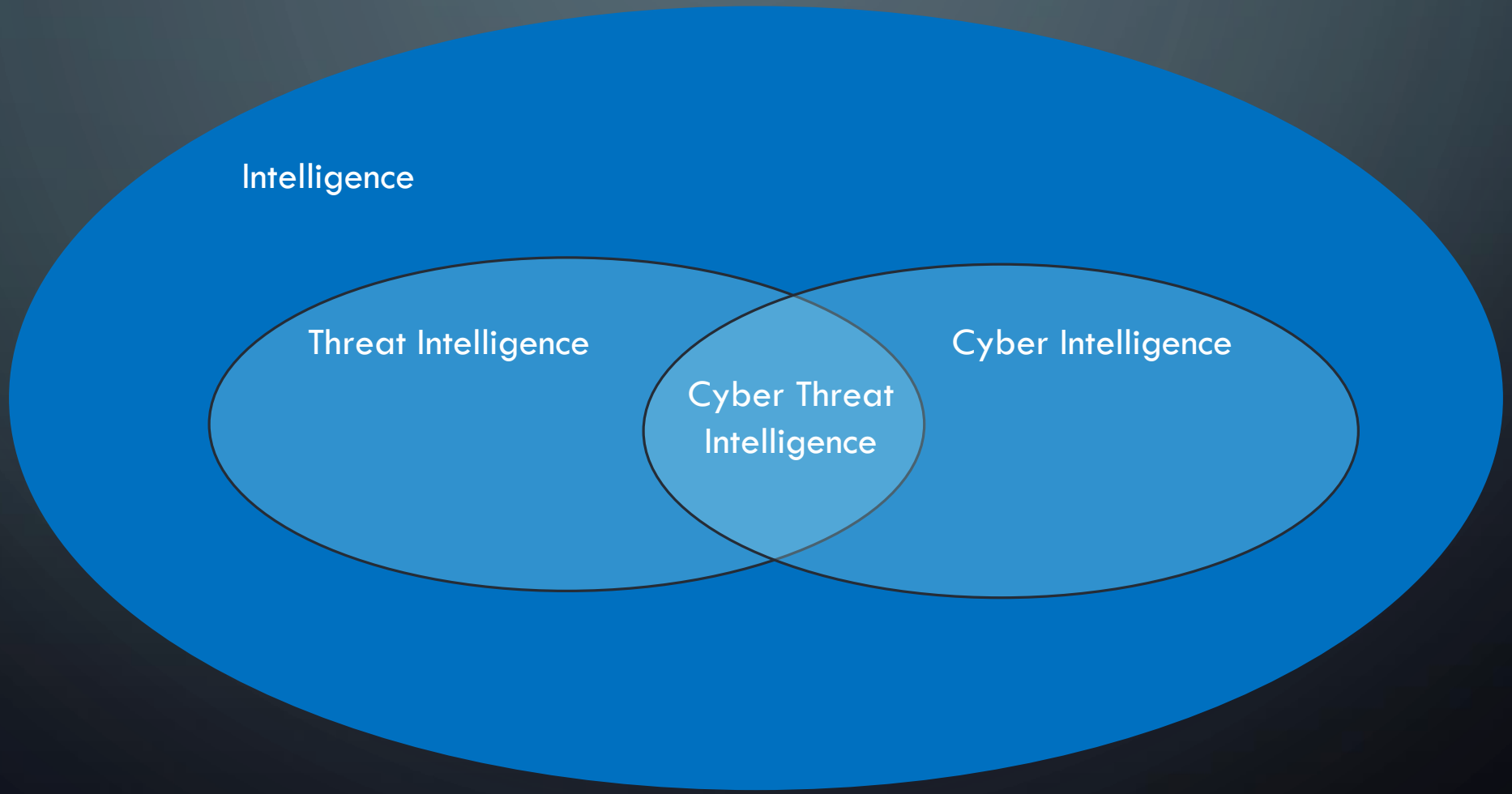
driven by curiosity

 # https://www.linkedin.com/in/cristicalita/

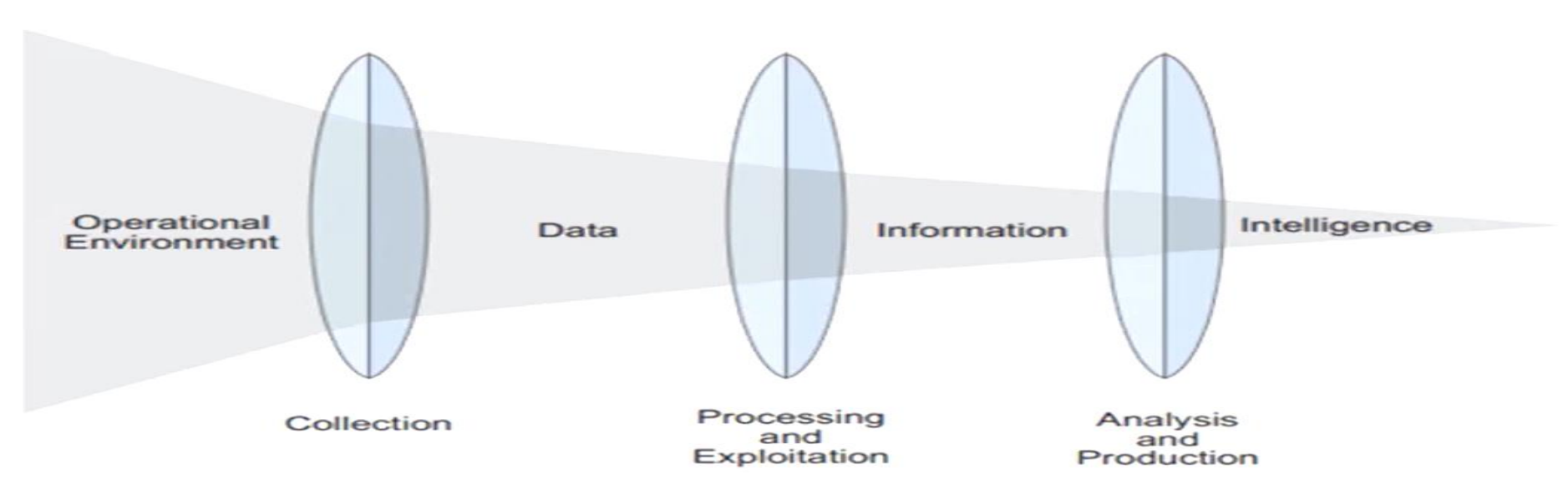
_MAIN OBJECTIVES

- Bring this activity field into the spotlight.
- Share a view on CTI activity and on a regular CTI process.
- Share few challenges that CTI Teams are currently encountering.

INTRODUCTION – STATEMENT 1



INTRODUCTION – STATEMENT 2



IP1
IP2
IP3
.
IPn

IP1 and IP 3 have a bad reputation

IP 1 and IP3 are C&C servers used by group X in campaign Y

Image source: https://digital-forensics.sans.org/blog/2015/07/09/your-threat-feed-is-not-threat-intelligence/

_INTELLIGENCE GENERATION VS CONSUMPTION

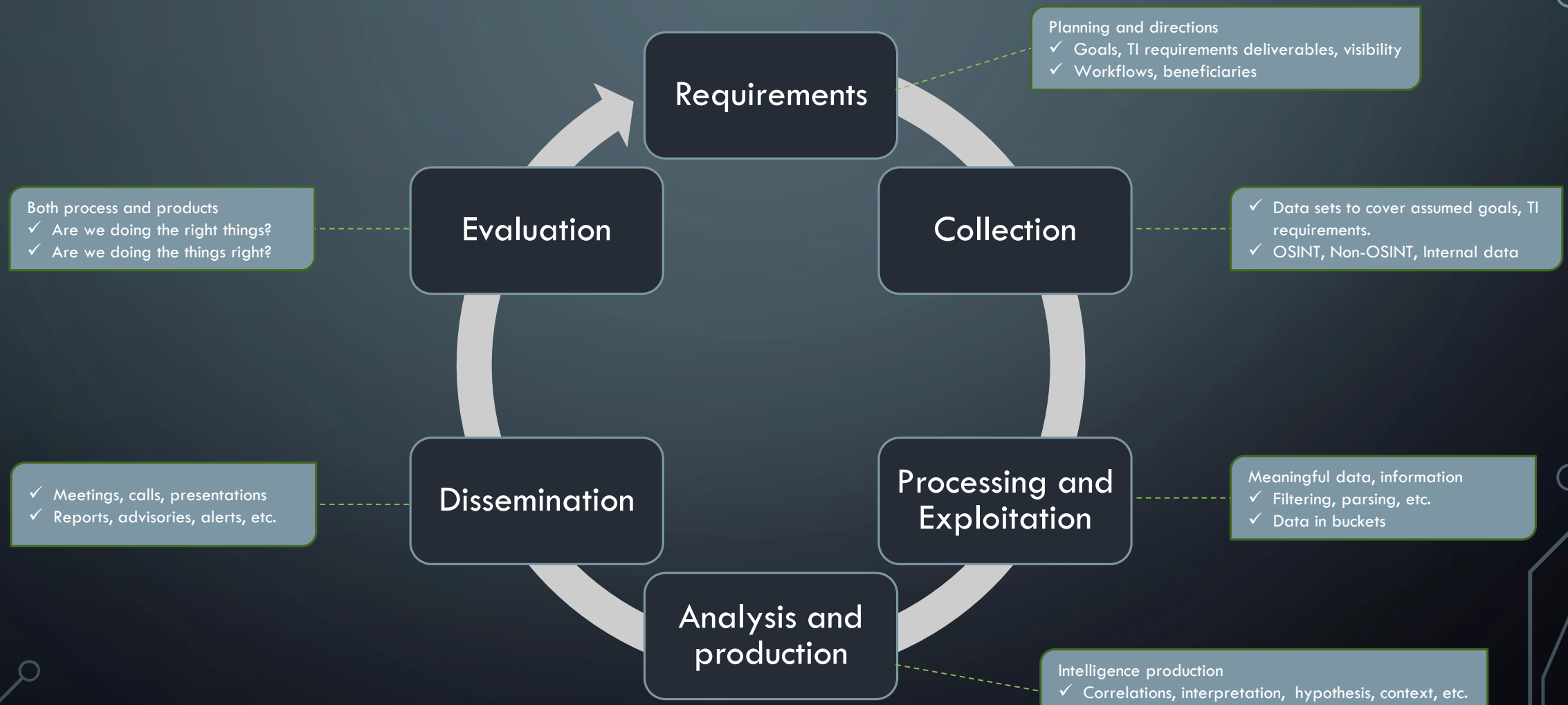
_generation

- This is based on the analysis of internal intrusions;
- It is used to discover, analyze and understand campaigns against your organization;
- It requires a fair amount of data to be collected – the results will be depending on the collection analyzed;
- It uses models and processes as Cyber Kill Chain, Diamond Model, etc.
- This is mostly seen at the security service providers level.

_consumption

- This is what the most organizations wants
- The TI team will have to understand intelligence and to know the organization's cyber battlefield;
- This is based on the internal and external collections;
- The TI analyst will filter huge amounts of data sets, will analyze it and will extract and direct the intelligence to the right people in the organization.

CYBER THREAT INTELLIGENCE – PROCESS & PRODUCT

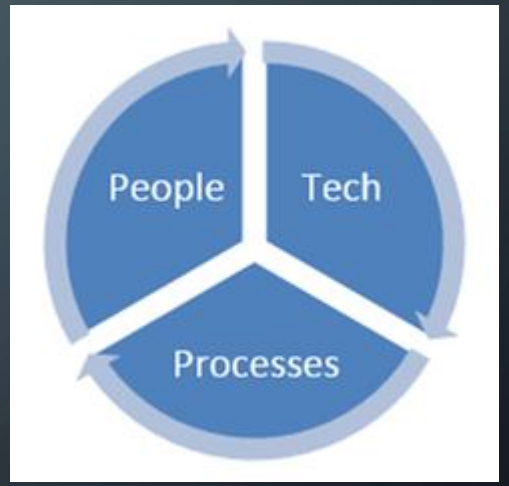


KEY ELEMENTS IN THE CTI ACTIVITY

People – people having the right skills and knowledge, on the right positions

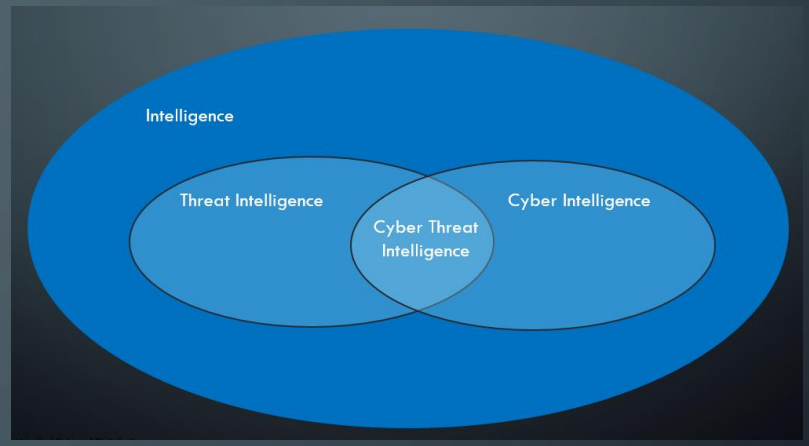
Processes – the defined and agreed flows to act upon in order to achieve a goal.

Technology – technological means to support and make the activity more efficient.



CAN'T HELP 1

Cyber Threat Intelligence ≠ Cyber Security



Why:

- Misunderstanding CTI
- Unclear purpose, roles and responsibilities

CAN'T HELP 2

…if people in senior/executive positions don't care about threats or they care about all threats

What could possibly go wrong?

CAN'T HELP 3

…stingy and greedy.

A mature CTI program will need adequate resources.

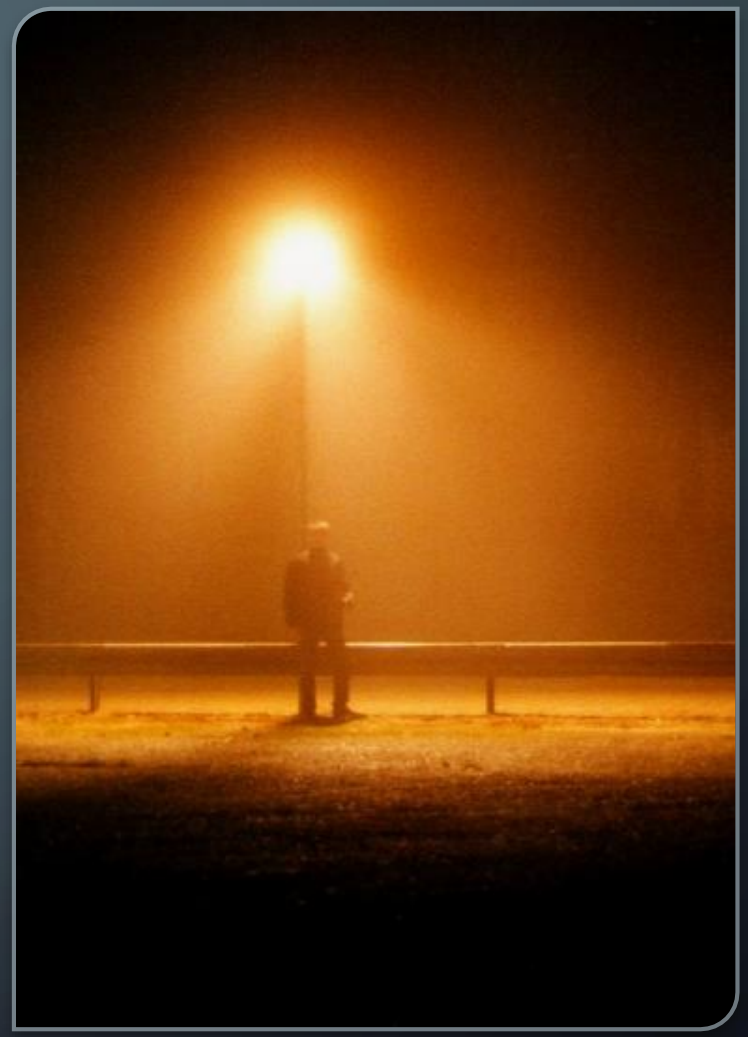
- Time
- Money

It is a challenge to demonstrate the ROI. And to implement metrics.

CAN'T HELP 4

…if no/low visibility and authority is granted to CTI Team.

- Internal and external
- Deliberately or due to internal issues



CAN'T HELP 5

…when wrong people are in the driver seat

- During program's lifecycle
- In the CTI Team

_ANCIENT CYBER WISDOM – PRESENTATION TAKE AWAY

“ The opportunity of defeating your enemy is provided by the enemy himself – the only thing you need is to have it pointed out by your Cyber Threat Intelligence Team”

Sun Cyber Tzu