# Συγκέντρωση Πληροφοριών

## Anticipating Surprise – Fundamentals of Intelligence Gathering

Fred Donovan
*NY/NJ Chapter*
*Twitter: kcfredman*
fred.donovan@owasp.org

“I do not War against walls”
Aodh Mór Ó Néill - 1601

(Literally Hugh “the Great” O’Neal)

# Fred Donovan @kcfredman

OWASP NY/NJ

Developer/Hacker/Intelligence Analyst

Guitarist: OWASP Band (on tour now)

12 yrs Freelance Public/Private Industry

Husband, Father, Brother to Many

# Intelligence is about Conflict
# It is not about being right or wrong

Conflict has three areas of capacity

- Prevention
  - Making an existing situation more advantageous
- Deterrence
  - When preventive measures fail
- Defeat
  - Resolving an intrusion in a custom way

# Four True Sources of Intelligence

Basic Rule of strategic conflict: The offense **always** wins

- Open Source
  - Overlooked but valuable (published and unpublished)
- HUMINT
  - Making an existing situation more advantageous
- COMINT
  - When preventive measures fail
- Cyber Collections
  - The offense always wins

# Four True Sources of Intelligence

Basic Rule of strategic conflict: The offense **always** wins

- Open Source
  - What is said is not as important as who said it
- HUMINT
  - Dealing with illicit networks (commercial espionage) Elicitation is hearsay
- COMINT
  - Generally illegal for private entities
- Cyber Collections
  - Hack thineself and to thine ownself be true.

# Definitions from an Intelligence Perspective

## What is data?

- Data is the “Individual observations, measurements, and primitive messages from the lowest level. Human communication, text messages, electronic queries, or scientific instruments that sense phenomena are the major sources of data.”

## What is Information?

- Information is “Organized sets of data…The organizational process may include sorting, classifying, or indexing and linking data to a place data elements in relational context for subsequent searching and analysis.”

# Definitions from an Intelligence Perspective

## What is Knowledge?

- Knowledge is information "…once analyzed and understood." This is where comprehension takes place when utilized both the static and dynamic relationships of the objects of data and the ability to model structure past (and future) behavior of those objects. (Referred to as Intelligence in the military).

# There is a difference between Data and Information

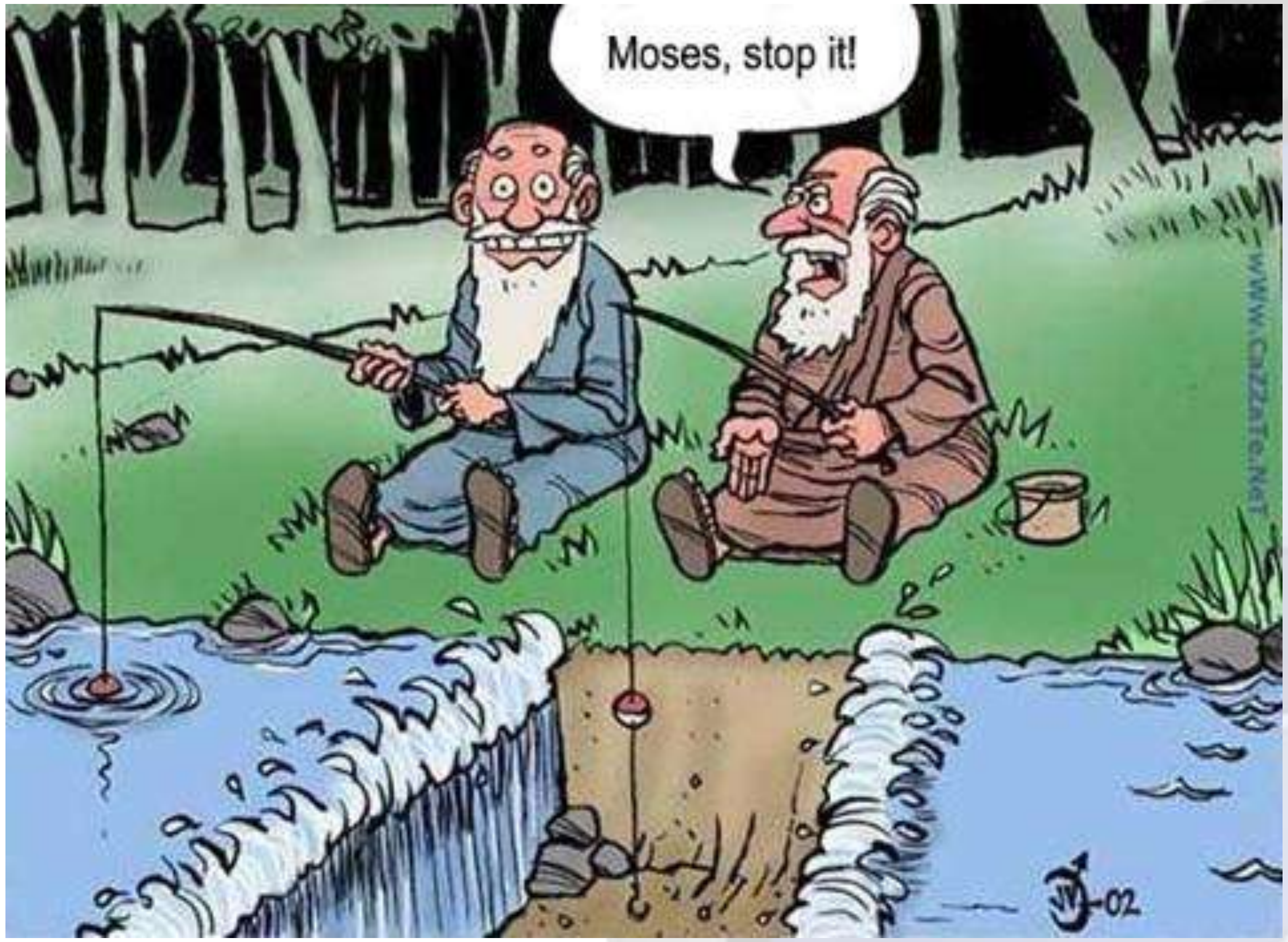
Data is unprocessed fact or fiction

Information is “validated Data”

# Classical Theatre of Historical Intel

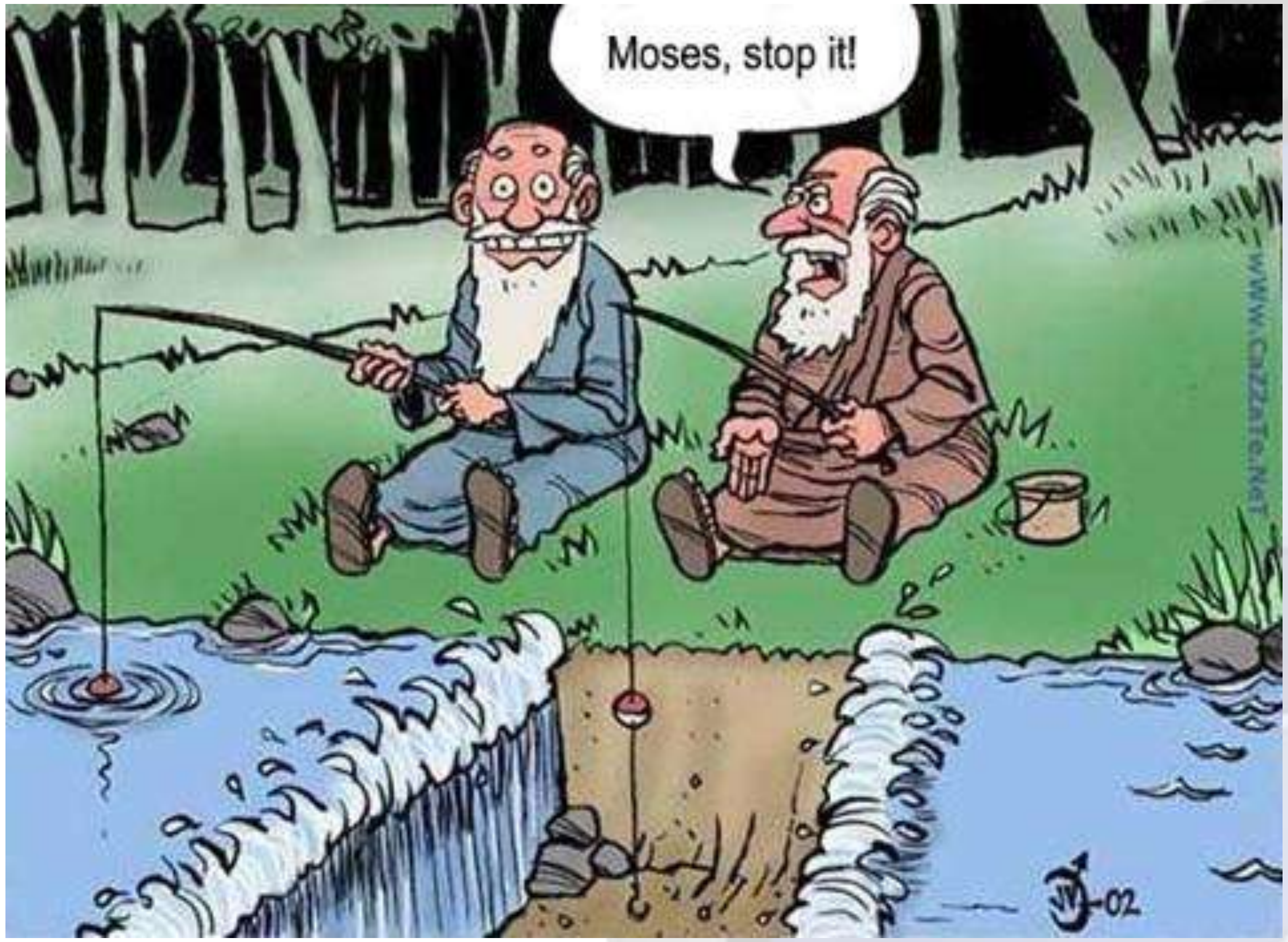
A small collections of historical successes and fails

# Moses: The First Operations Director of Intelligence



Sent spies into Canaan for clandestine intelligence

# Moses: The First DMZ



Of the 12 tribes of Israel, one was not commissioned for war. The Levites were appointed rather than counted.

# Maghreb: Islamic caliphates

The expansion of Islamic Influence

5 million square miles

# Maghreb: The First Firewall

The Sahara: Host and Perimeter

# Hugh O’Neill and Elizabeth 1

Social Intelligence

# Hugh O’Neill and Elizabeth 1

Fighting the enemy with a proverbial Virus of humans

# Some basics on Intelligence Gathering

## Precision

- Understanding the problem accurately and in details
  - Design the problems in detail
  - Cyber attacks evolve and modify accuracy and dimensions of Information
- Stakeholders value the abstract of linkages

# Some basics on Intelligence Gathering

## Evaluation and Criteria

- Too much subjectivity in collections
- Evaluate the sources of information
  - Every source has motives
  - Determine the bona fides
- Evaluate the communications channel

# Some basics on Intelligence Gathering

## Evaluation and Criteria – cont.

- 2nd law of thermodynamics (Entropy)
- Info on attacks is often from secondary sources and reliability in your organizations may suck as well.
- Use proper communications channels.
  - OWASP
    - SQL Injection Attacks and Defense – Sir Justin Clarke

# Some basics on Intelligence Gathering

## Evaluation and Criteria – cont.

- Use proper communications channels - cont.
  - OWASP
    - Teams of people with like expertise but diverse skills on subject matter
    - SQL Injection Attacks and Defense – Sir Justin Clarke – multiple contributors
    - OpenSAMM – by Pravir, yet influenced by Gary McGraw and Dan Cornell

# Some basics on Intelligence Gathering

## Destruction and Analysis

- Deconstruct the highest level of abstraction into the lowest levels of tasks
  - KIQ’s and EEI’s – Key intelligence questions and essential elements of information
    - Targets of Analysis – the attackers and methods

# Some basics on Intelligence Gathering

## Destruction and Analysis – cont.

- KIQ’s and EEI’s – cont.
  - Operations of Analysis
    - HUMINT, COMINT, etc.
  - Linkages

# Some basics on Intelligence Gathering

## Model the Intelligence

- Anybody heard John Steven talk of Threat Modeling???
- An illustration of collected intelligence into a model
- Extract information from the Model
- Draw conclusions

# An Idea

Warning is cumulative and not merely current.

"The ultimate goal of Stratagem is to make the enemy quite certain, very decisive and wrong," Barton Whaley

# Thank you

fred.donovan@owasp.org
@kcfredman

???

# Feedback Please.

https://www.surveymonkey.com/s/Research12_FredDonovan