



# Cyber Threat Intelligence

---

# Aims

---

- Understand the need for CTI
- Understand the foundations of CTI
- Understand the building blocks of CTI

# Introduction

---

- How can you know the risk without knowing the threat?
- Threat assessment is the bed rock of a good risk assessment
  - Allows you to explore who/what might be after you
  - Informs the risk analysis process

# Threats

---

- Threat = those things that may pose a danger to your information security
- Threat Actor is the agent that poses the threat
  - Can be malicious or accidental
  - Have the opportunity and capability to exploit a vulnerability

# Threat Assessment

---

- Threat assessment identifies the threats to the organisation
- Identifies the likely culprits
- Threat assessment in this space is not very mature
  - Often borrows from other environments/domains
  - Difficult to provide quantified, accurate and repeatable outcomes

# Background

---

- Threat assessments were regularly carried out by nation states on other nation states
  - Later businesses started to apply techniques for the market place
- National threat analysis done by experts
  - Normally considered over lengthy periods
- Threat Analysts will tend to specialise in specific parts of the threat spectrum, geographical region etc.

# Time Period

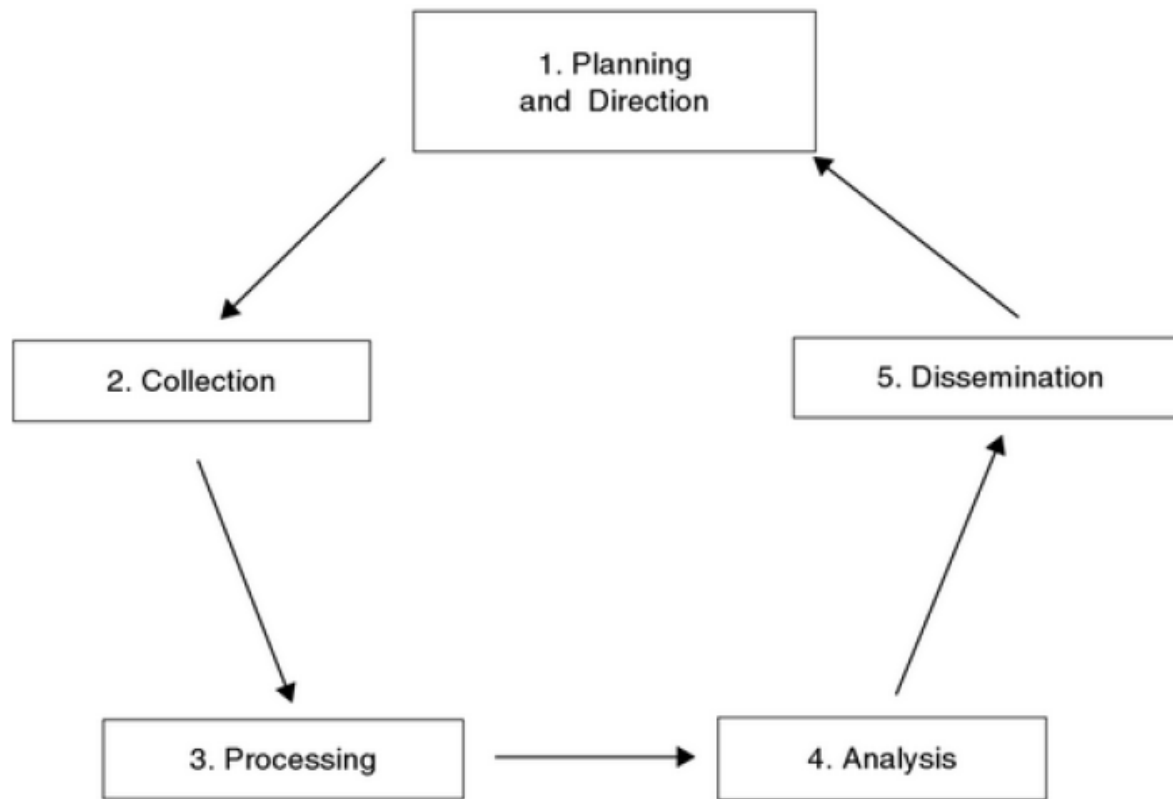
---

- State threat analysis normally has a long time period to make assessments
- State attacks are normally a lengthy diplomacy phase coupled with a military build up
- Terrorist attacks may not have a diplomacy phase but still need planning and deployment
- Cyber attacks have short timescales
  - Build up maybe unobservable
  - Lower threshold to initiate
  - No requirement to move physical resources
  - Can attack from any location
  - Limited observable indicators
  - 1 attacker has all that they need



# Creating Intelligence

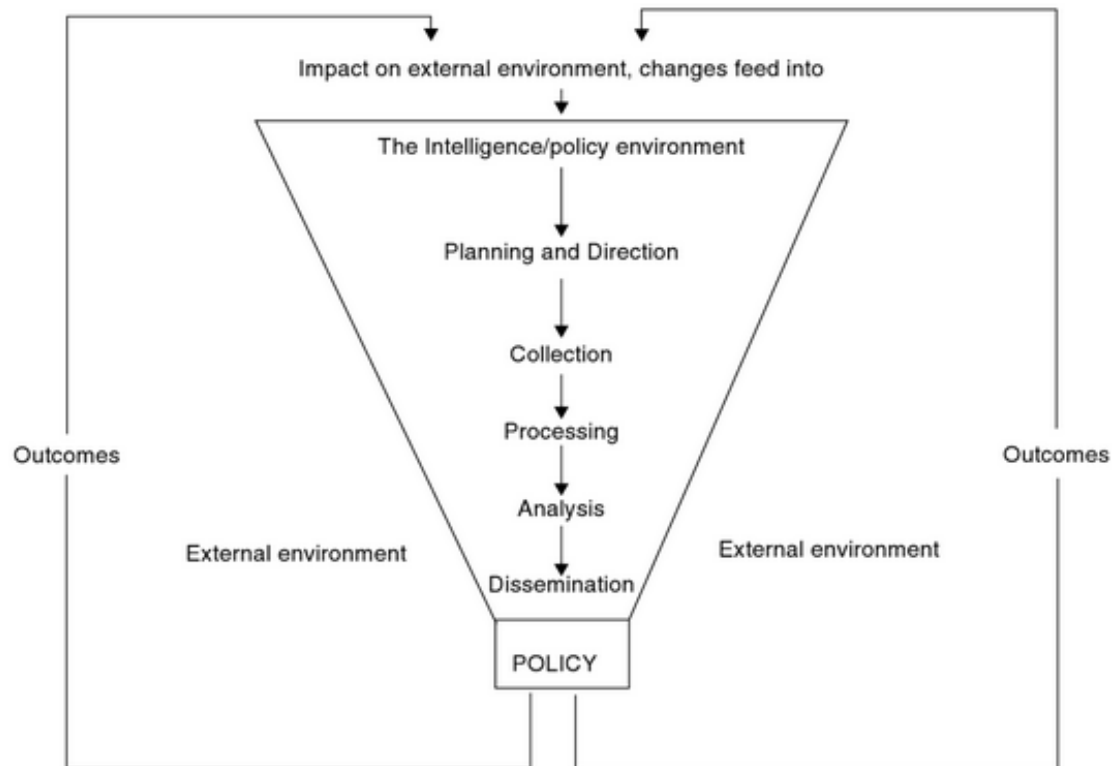
---





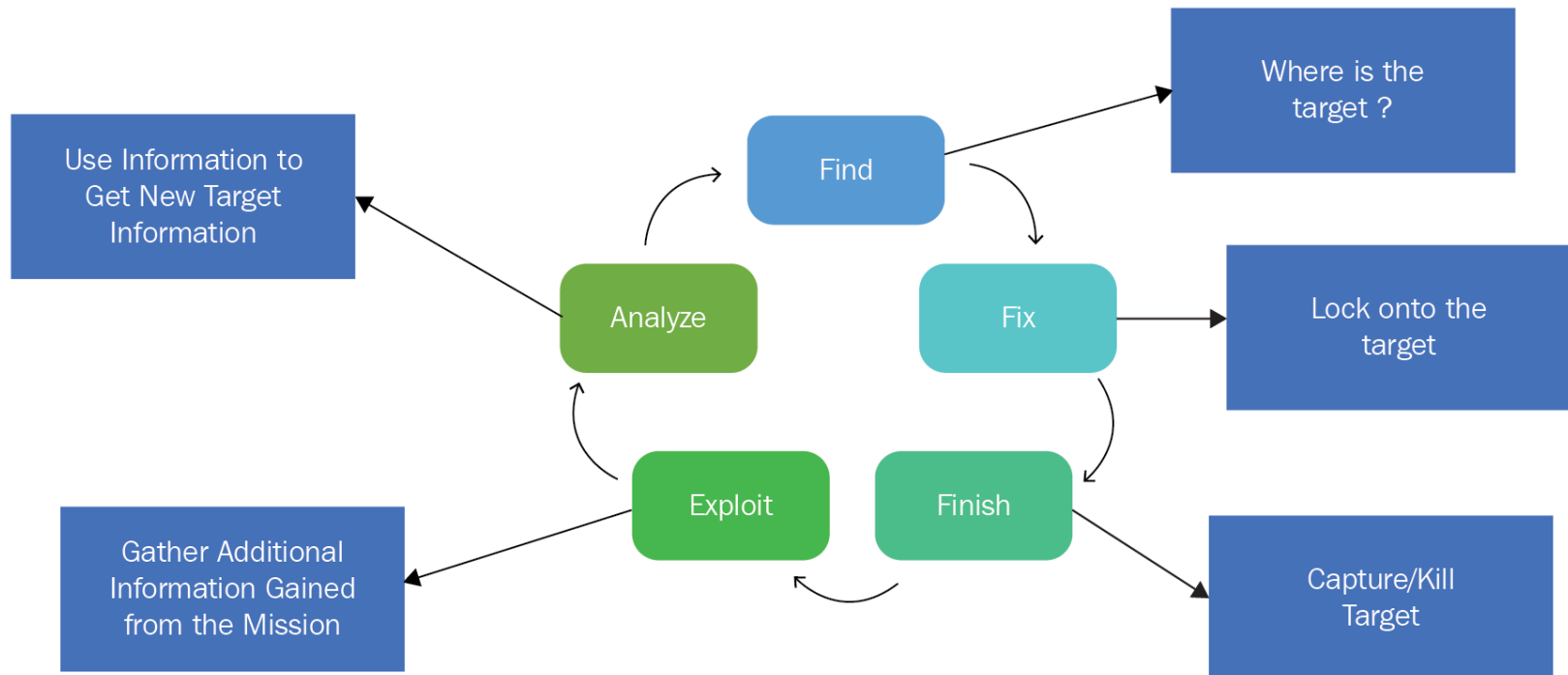


# The Intelligence Funnel



# F3EAD

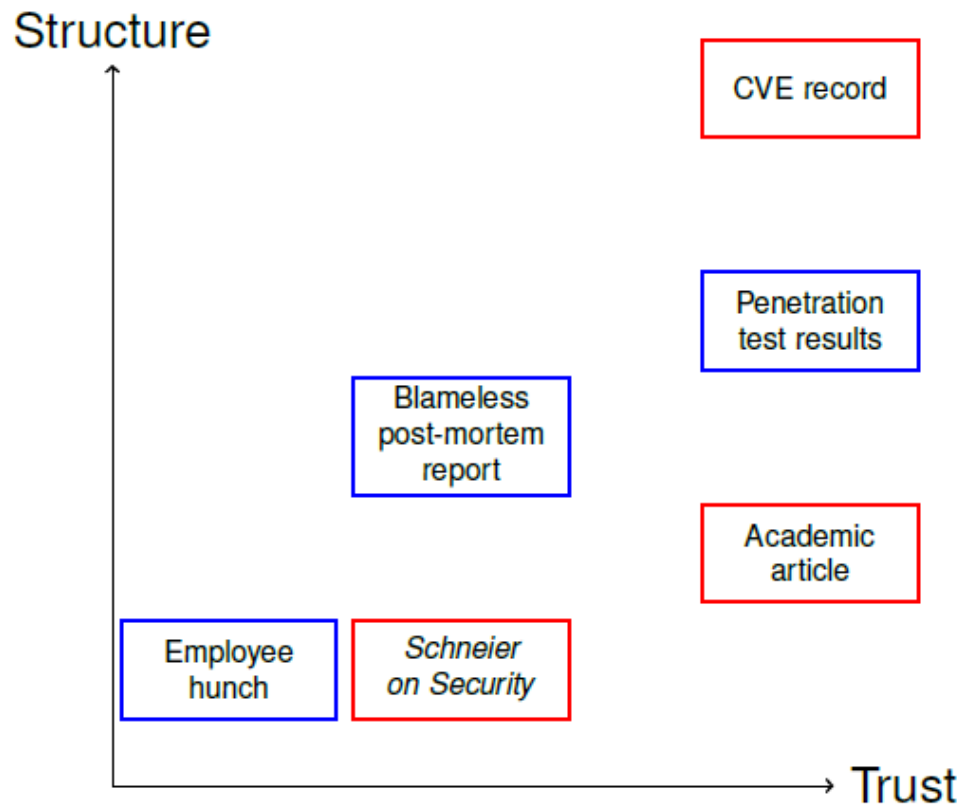
## Military Targeting Process



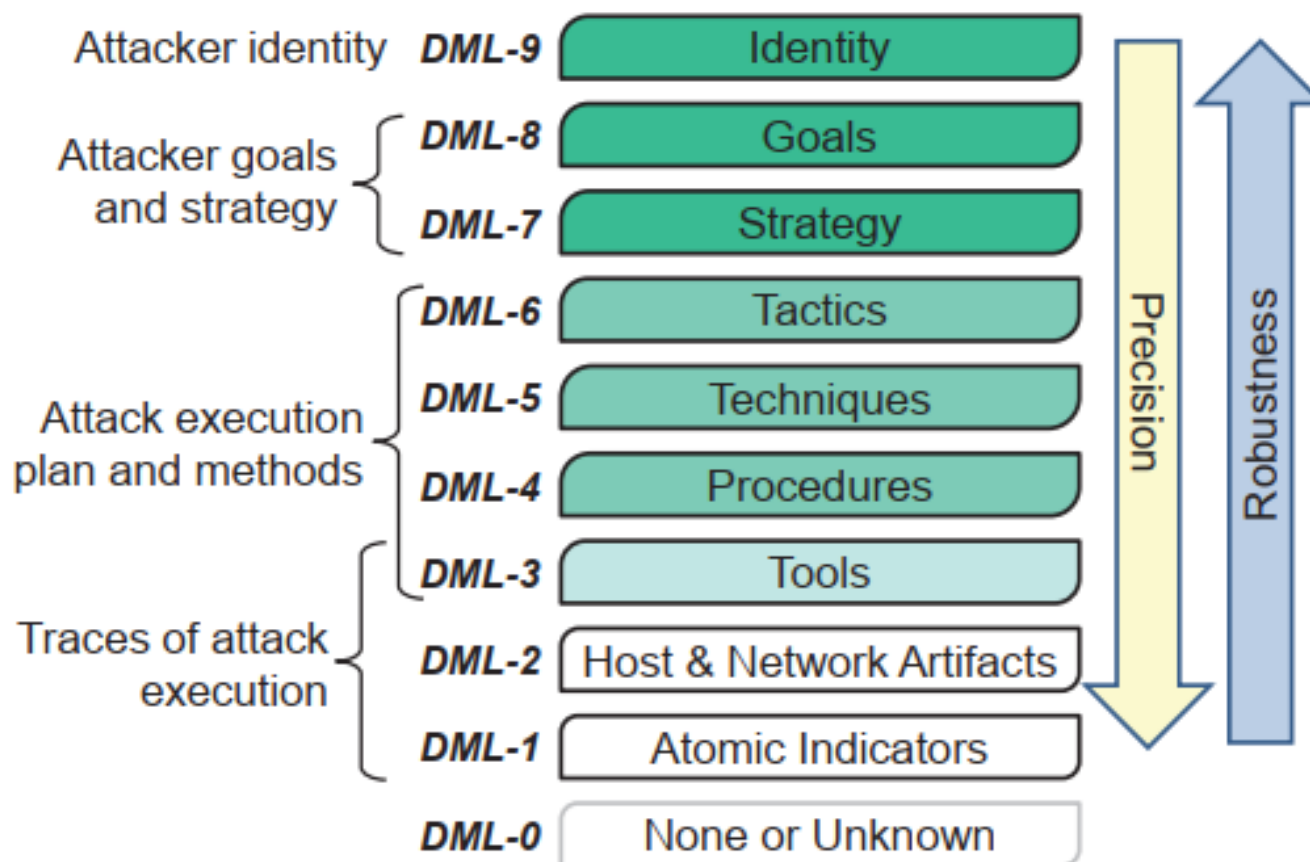


# Data Sources

---



# Maturity





# Questions?

---

# References

---

- Wiem Tounsi and Helmi Rais. 'A survey on technical threat intelligence in the age of sophisticated cyber attacks'. In: Computers & security 72 (2018), pp. 212–233.
- Peter Gill and Mark Phythian. Intelligence in an InsecureWorld. Second. Polity Press, 2012.
- Gragido, Will (October 3, 2012). "Understanding Indicators of Compromise (IoC) Part I". RSA. Archived from the original on September 14, 2017. Retrieved June 5, 2019.
- Peter Gill. 'Theories of intelligence: Where are we, where should we go and how might we proceed?' In: Intelligence Theory: Key Questions and Debates. Routledge, 2008, pp. 208–226.
- CIA. The Intelligence Cycle. 2001. <https://fas.org/irp/cia/product/facttell/intcycle.htm> (visited on 11/11/2019).
- Wilson Bautista Jr. Practical cyber intelligence: how action-based intelligence can be an effective response to incidents. Packt Publishing Ltd, 2018.
- Henry Dalziel. How to define and build an effective cyber threat intelligence capability. Syngress, 2014.
- Sherman Kent. 'Words of estimative probability'. In: (1964).
- ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends. ENISA, 2019.
- Ryan Stillions. The DML Model. 2014. URL: [https://ryanstillions.blogspot.com/2014/04/the-dml-model\\_21.html](https://ryanstillions.blogspot.com/2014/04/the-dml-model_21.html) (visited on 11/25/2019).
- Siri Bromander, Audun Jøsang, and Martin Eian. 'Semantic Cyberthreat Modelling.' In: STIDS. 2016, pp. 74–78.