# ENISA CTI – EU Event

# Bonding EU Cyber Threat Intelligence

## 30-31 October 2017, Rome

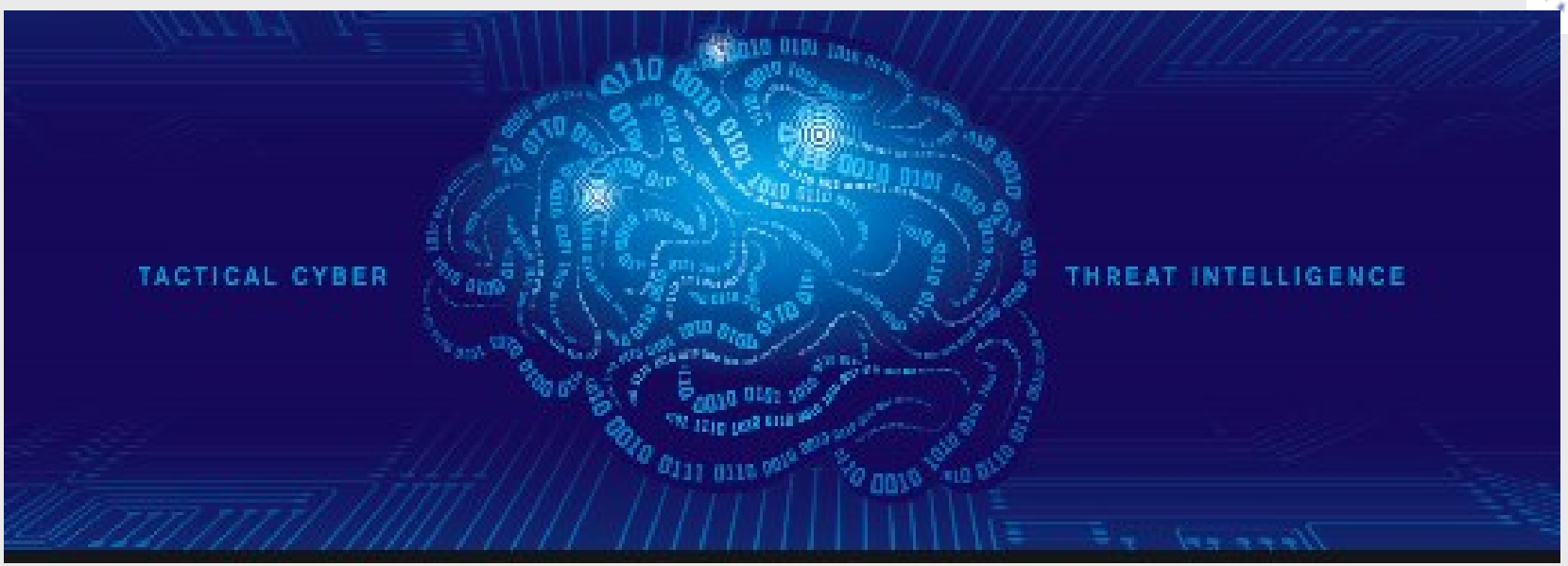
The event is organized in cooperation with:

DG Connect/H1

Europol EC3

CERT-EU

European Defence Agency




# Embedding CTI in security organisation

***Use CTI to improve your (security) processes***

Paul Samwel

# Format

4 talks TED style:

20 minutes presentation

15 minutes questions & discussion

BREAK

pitches from the audience (no slides needed)

6 minutes pitch

4 minutes questions & discussion on pitch

Group discussion on CTI for improving your security organization

# Agenda

**9:00 Introduction (Paul Samwel)**

**9:10 Using CTI for prioritizing security improvements (Paul Samwel)**

**9:45 Scaling Intelligence for Communities (Chris O'Brian)**

**10:20 Translating Intelligence for the Business (Tierman Connolly)**

**10:55 CTI capability framework (Richard Kerkdijk)**

**11:30 Break**

**12:00 Pitches from the audience.**

- Human behaviors and the Cyber Kill Chain (Michael Meijerink)
- <pitch 2>
- <pitch 3>
- <pitch 4>
- <pitch 5>

**13:00 Lunch**

**14:00-16:30 Plenary session with summary of our discussions**


# Using CTI for prioritising security investments

Paul Samwel, October 2017

# Paul Samwel

NOREA
de beroepsorganisatie van IT-auditors

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

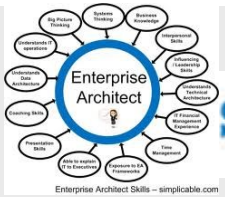
ENISA
CURRENT THREAT LANDSCAPE EMERGING
ETL 2015

CyberCrime Task Force


EY




Rabobank




SecurityInnovation

# Problem

***Cybercrime resilience requires  Multiple layers of security***

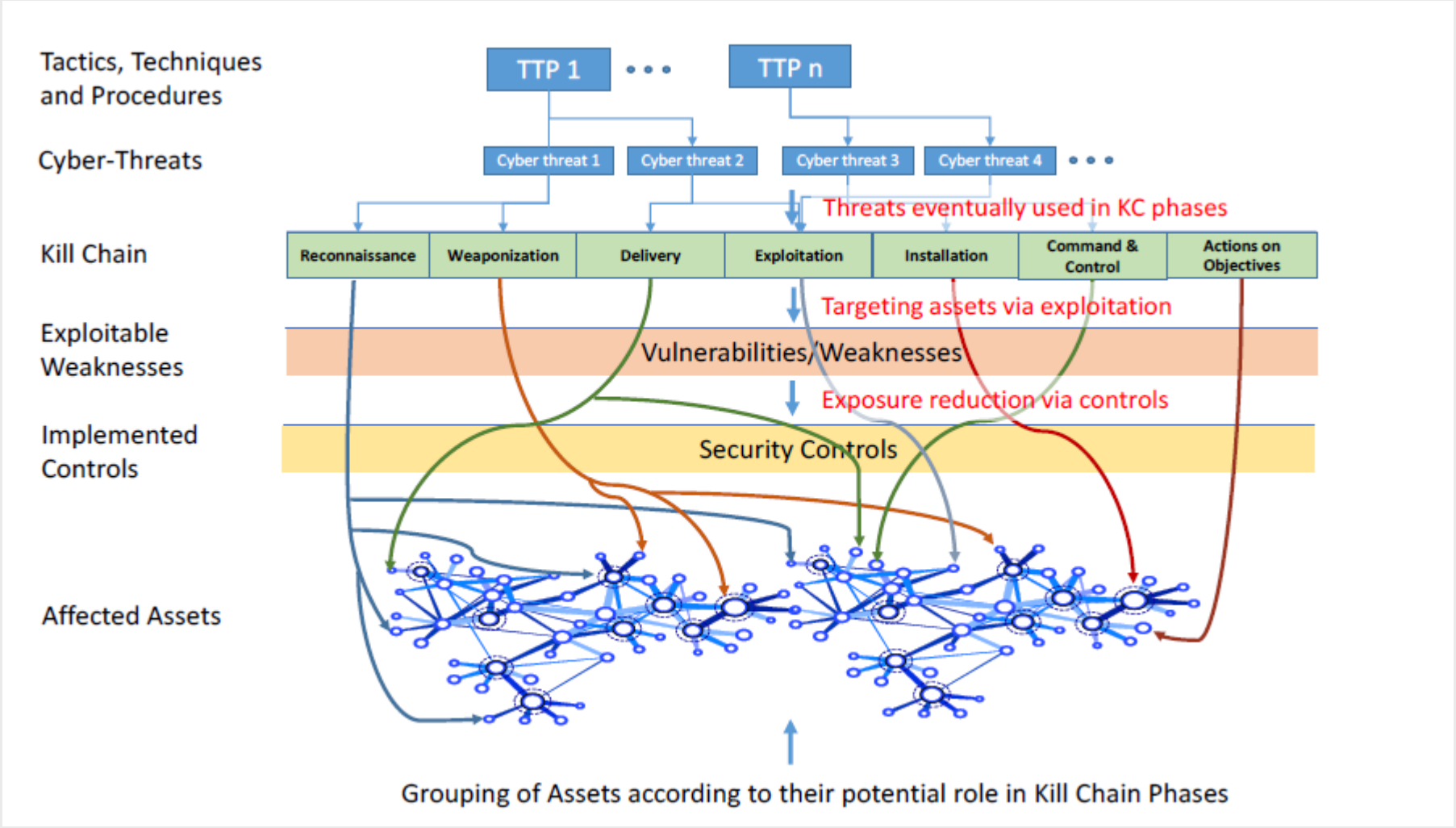

***How to prioritise your security investments?***

# Solution:
# Use the Cybercrime Kill Chain

Cyber Threat Intelligence


Priorities

# 1. Find your "crown jewel" assets



# 2. Use CTI to find relevant Modus Operandi for your crown jewels

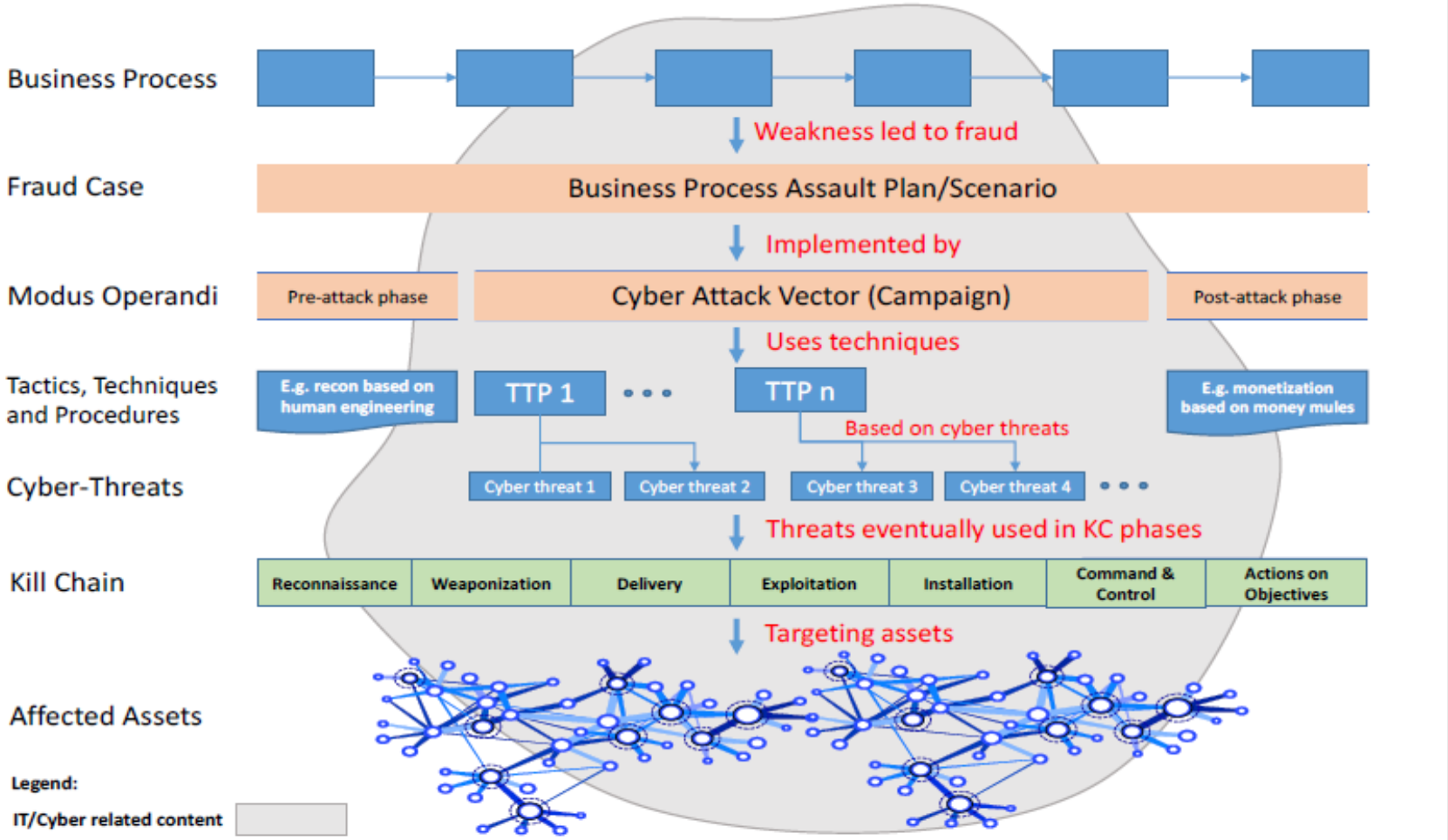
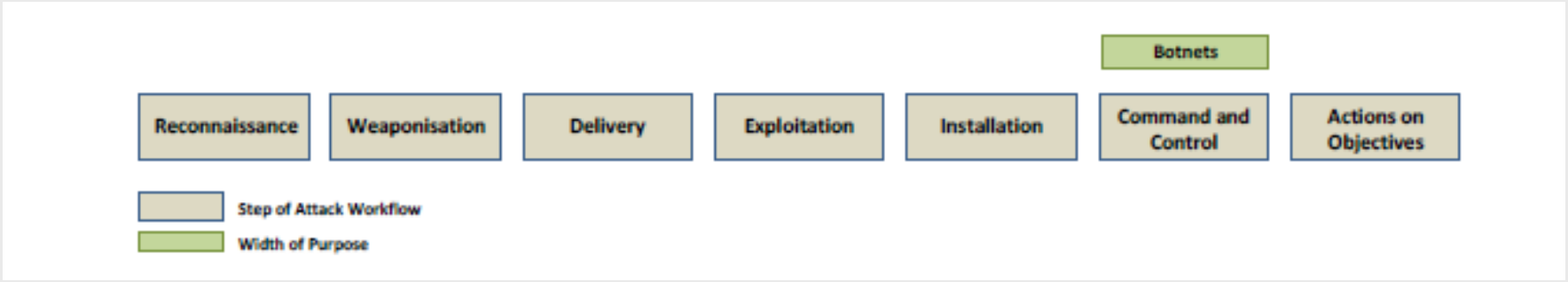



Figure 2: Big picture CTI elements from Modus Operandi to affected assets

# 3. Find common attack steps in those MO's




# 4. Find controls to break (business case of) common attack steps

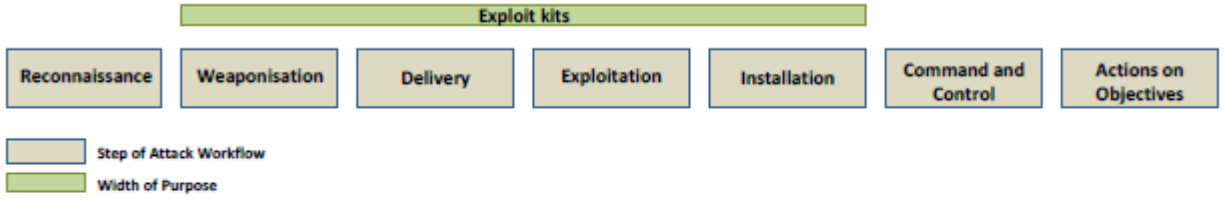



Figure 15: Position of Exploit kits in the kill-chain

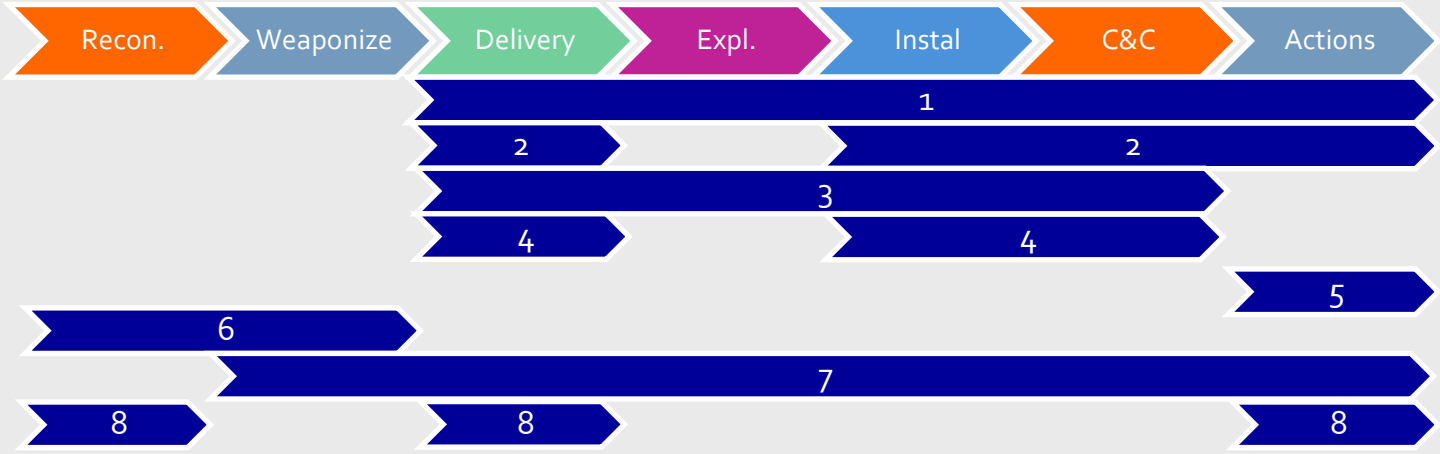
**Mitigation vector**: Exploit kits are infecting systems based on their vulnerabilities. Exploit kit themselves are installed as malware. Hence the mitigation vector for this threat contains elements found in malware:

- Performance of updates in a regular basis in orchestration with vulnerability management.
- Malware detection should be implemented for all inbound/outbound channels, including network, web and application systems in all used platforms (i.e. servers, network infrastructure, personal computers and mobile devices).
- Use of a security e-mail gateway with regular (possibly automated) maintenance of filters (anti-spam, anti-malware, policy-based filtering), as well as content filtering to filter out unwanted attachments, mails with malicious content and spam.
- Follow various vendor good practices[213].

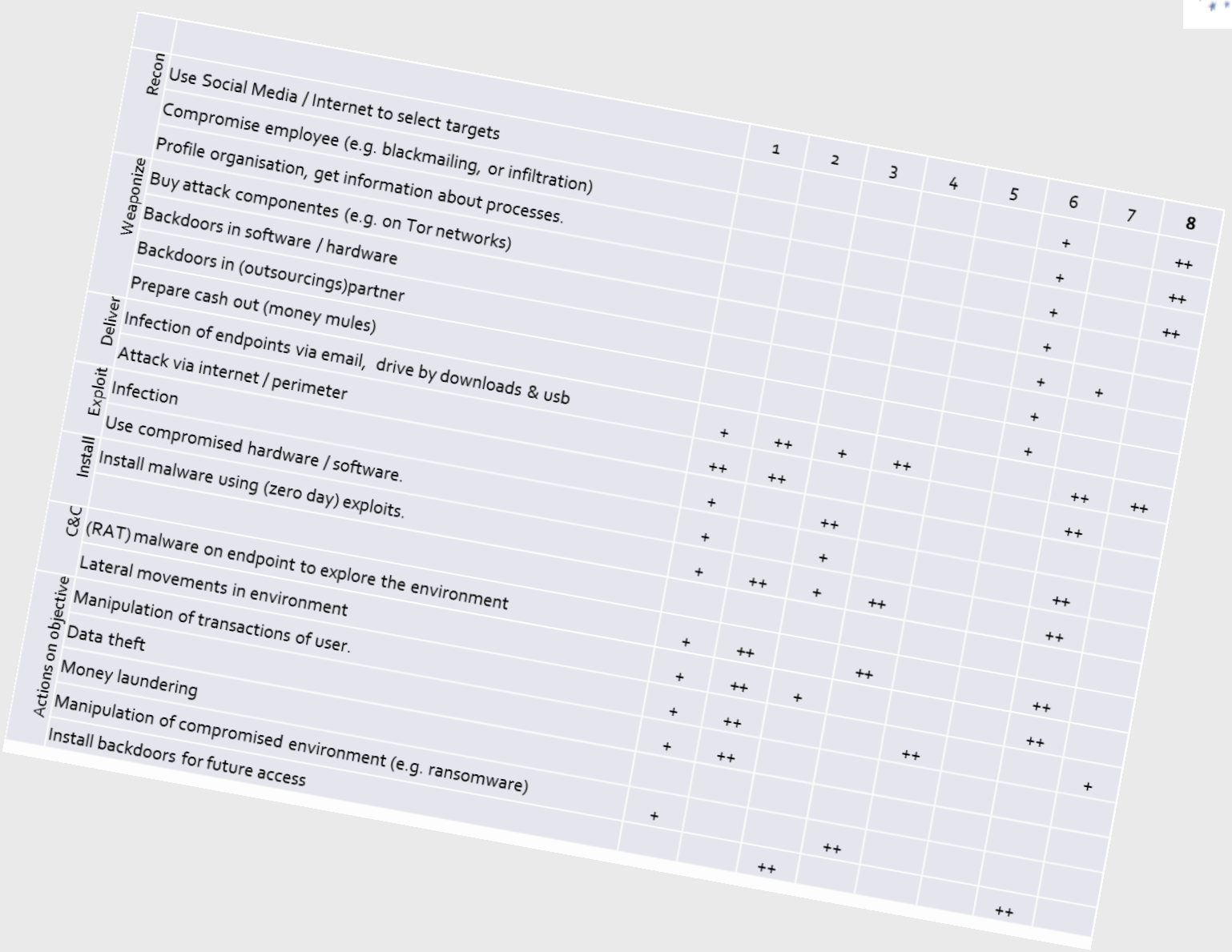
# 5 Check completeness by linking solutions to kill chain

## Controls

1. *Network segmentation in security zones*
2. *White listing and (anomaly) detection between zones*
3. *Anomaly detection within zones*
4. *Segmentation within user device based on risklevel*
5. *Signing of critical transactions by users within applications*
6. *Security Intelligence*
7. *Automated handling of IOC's*
8. *Awareness for employee*



# 6 check for blank spots

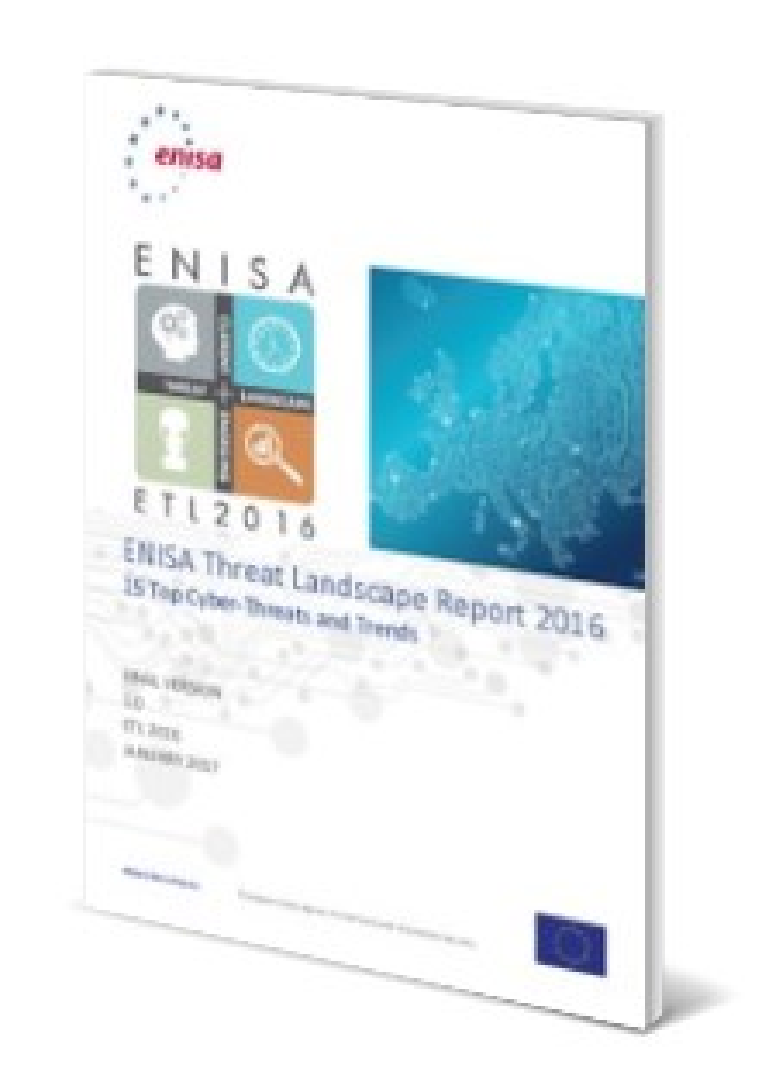


| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|---|
| Recon | Use Social Media / Internet to select targets | | | | | | + | | ++ |
| | Compromise employee (e.g. blackmailing, or infiltration) | | | | | | + | | ++ |
| | Profile organisation, get information about processes. | | | | | | + | | ++ |
| Weaponize | Buy attack componentes (e.g. on Tor networks) | | | | | | + | | |
| | Backdoors in software / hardware | | | | | | + | + | |
| | Backdoors in (outsourcings)partner | | | | | | + | | |
| | Prepare cash out (money mules) | | | | | | | | |
| Deliver | Infection of endpoints via email, drive by downloads & usb | + | ++ | + | ++ | | | | |
| Exploit | Attack via internet / perimeter | ++ | ++ | | | | | | |
| | Infection | + | | ++ | | | ++ | ++ | |
| | Use compromised hardware / software. | + | | + | | | ++ | | |
| Install | Install malware using (zero day) exploits. | + | ++ | + | ++ | | | | |
| C&C | (RAT) malware on endpoint to explore the environment | | | | | | ++ | | |
| | Lateral movements in environment | + | ++ | | | | ++ | | |
| | Manipulation of transactions of user. | + | ++ | + | ++ | | | | |
| Actions on objective | Data theft | + | ++ | | | | ++ | | |
| | Money laundering | + | ++ | | ++ | | ++ | | |
| | Manipulation of compromised environment (e.g. ransomware) | | | | | | | + | |
| | Install backdoors for future access | + | | ++ | | | | | |
| | | | ++ | | | ++ | | | |

# Summary

- ***The cybercrime kill chain can help you to find common attack steps.***
- ***By focusing your investments you will protect against multiple modus operandi.***
- ***Criminals tend to re-use attack steps. Hence you also protect against tomorrows modus operandi.***

# Further reading




https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016