**Objective of this framework: take the most important data from OSINT reports**

**1) CONTEXT**

*Date + security editor name + broad explanation of the malicious activity and eventually attribution*

***Analyst assessment:***

**2) VICTIMOLOGY**

- Type of industry:

- Geographical location:

**3) TOOLS**

- On the shelf:

- Custom:

**4) MITRE ATT&CK**

**Reconnaissance**

**Ressource Development**

**Initial Access**

**Execution**

**Persistence**

**Privilege Escalation**

**Defense Evasion**

**Credential Access**

**Discovery**

**Lateral Movement**

**Collection**

**C2**

**Exfiltration**

**Impact on Objective**

**5) IoCs**

- hash

- domains

- IPs

- hard-coded keys

- email address