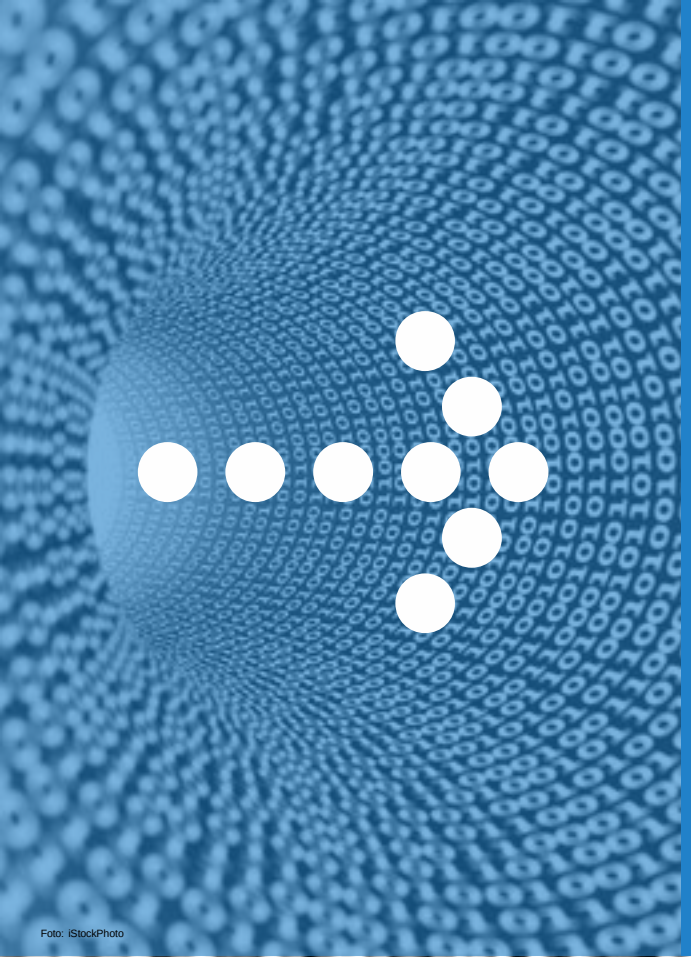


Foto: iStockPhoto

Development and evaluation of information elements for simplified cyber-incident reports

Patrik Lif, Teodor Sommestad & Dennis Granåsen

FOI

Information elements

- What information elements should be included in an incident report?

Background

Info. elements

Litterature

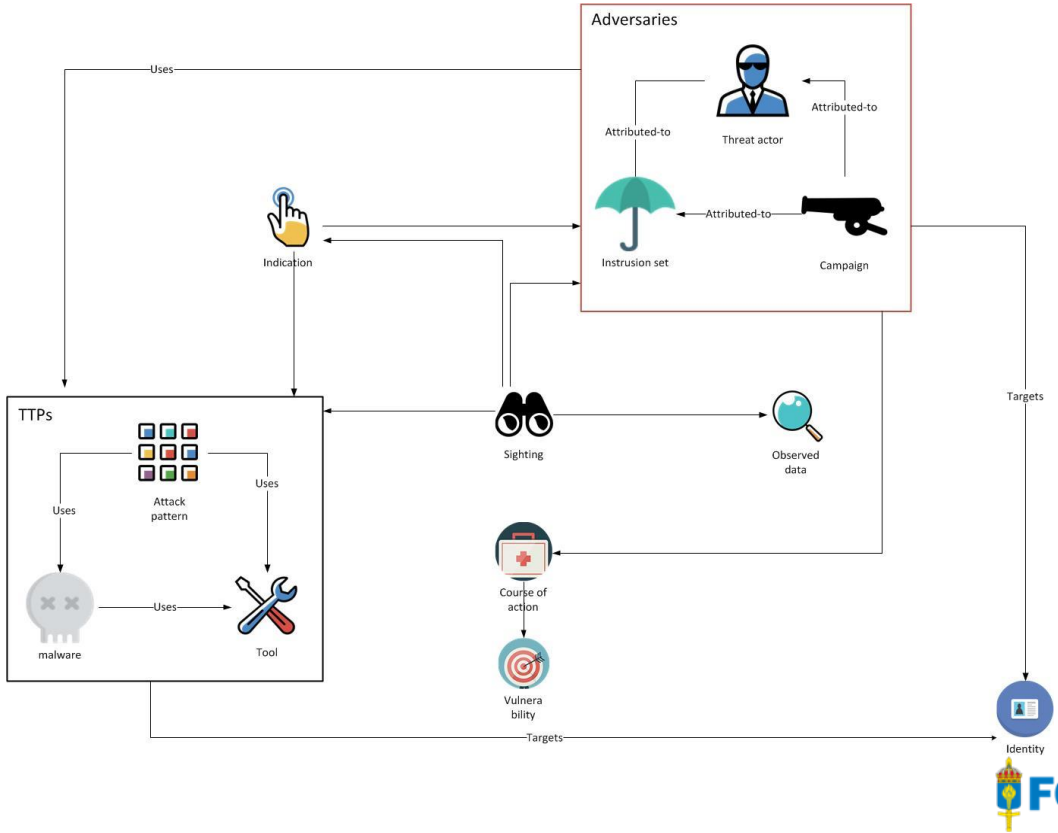
Frameworks

SA elements

Practical experiences

STIX - Structured Threat Information Expression

- Information sharing
- 178 properties + relations
- No description of own network



Information elements for simplified incident report

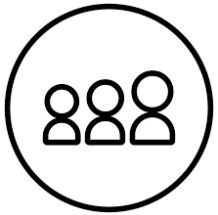
Background	Victim	Attacker	Incident description	Damage assessment
Rapporteur Observations/ indications	Node User Comment	Node User Comment	Suspected attack objective Attack or vulnerability details Attack mechanisms Attack domains	Probability that the attacker succeeded Asset criticality Attack impact Response urgency

iPilot – 4 day excercise

Participants (30)

Adversery (3)

Tech. support (5)



Staff (10)

Evaluation (7)

Visitors (65)

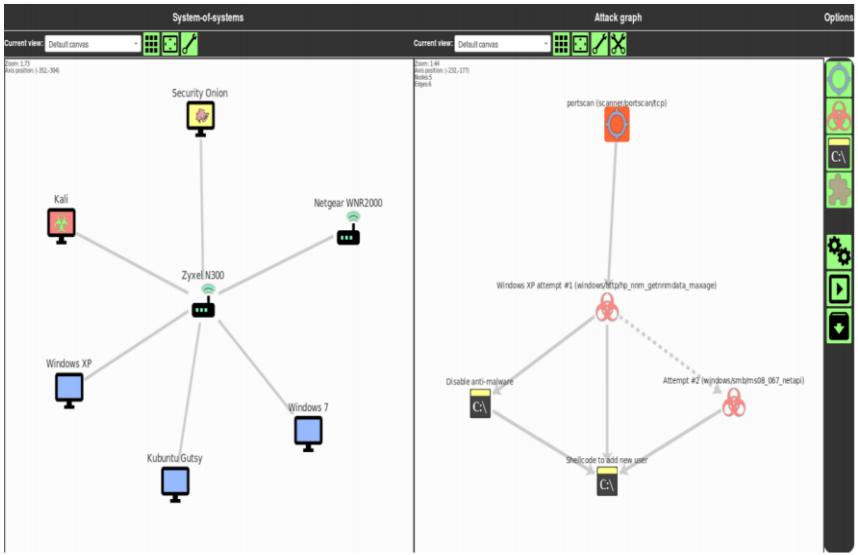
Attacks & tools

- µTorrent downloads malware.
- DDos attack.
- Similar Ukraine scada-attack.
- Unauthorized hardware.

- Analysis with Wireshark, ELK, Snort, and Windows Event Log to collect information in a central system.

CRATE & SVED

400 + 400 servers



iPilot - evaluation

Background | Victim | Attacker | Incident descr. | Damage assessment

Suspected attack objective

- ○ Obtain system privilegies (e.g. to remotely control a machine)
- ○ Obtain information (e.g. network scans or eavesdropping)
- ○ Influence a system's functionality (e.g. denial-of-service attacks)

Attack or vulnerability details

Describe the attack, e.g. by the CVE code of the exploited vulnerability.

Attack mechanism(s) believed to be used (from CAPEC)

- ☐ Collect and Analyze Information
- ☐ Inject Unexpected Items
- ☐ Engage in Deceptive Interactions
- ☐ Manipulate Timing and State
- ☐ Abuse Existing Functionality
- ☐ Employ Probabilistic Techniques
- ☐ Subvert Access Control
- ☐ Manipulate Data Structures
- ☐ Manipulate System Resources

Attack domain(s) believed to be concernced (from CAPEC)

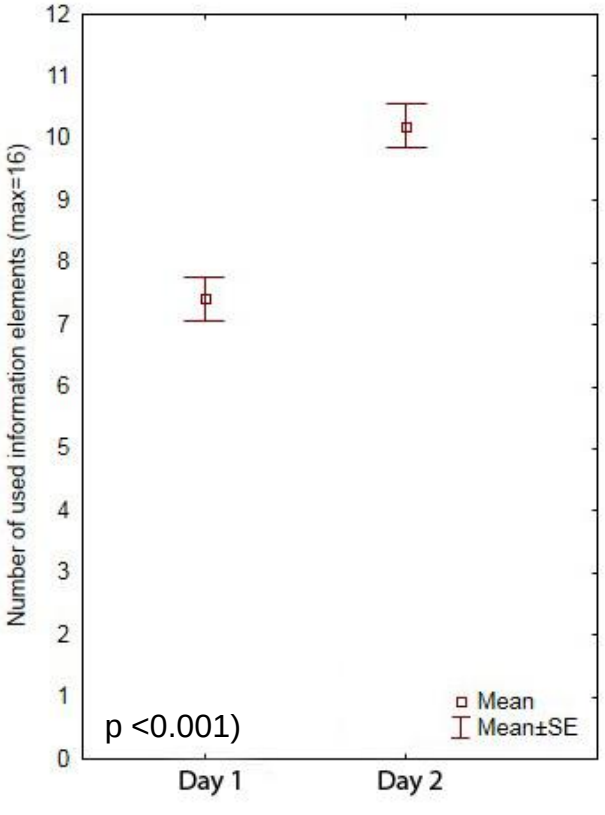
- ☐ Social Engineering
- ☐ Supply Chain
- ☐ Communications
- ☐ Software
- ☐ Physical Security
- ☐ Hardware

Purpose

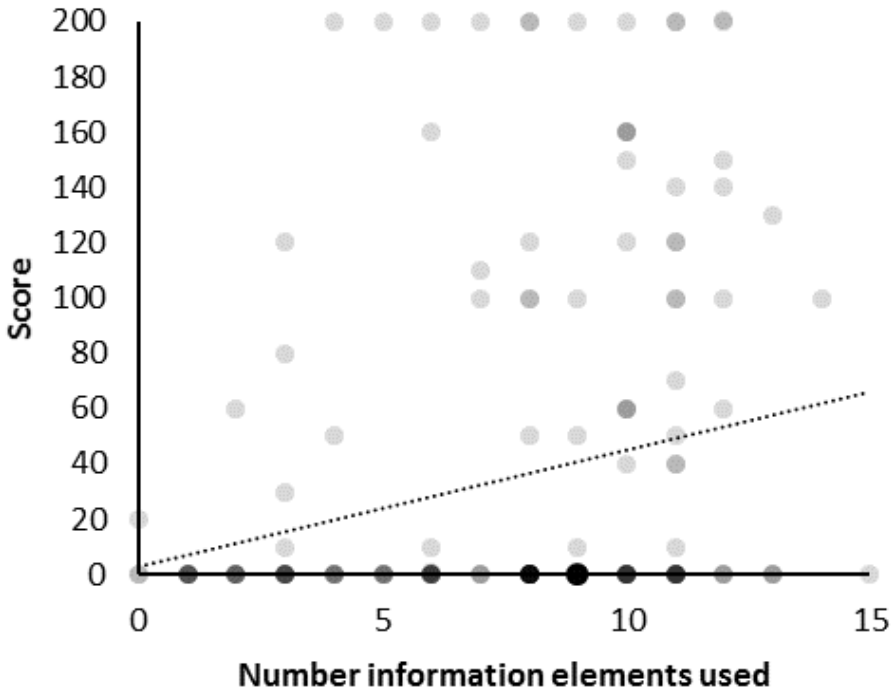
- Use of the 16 information elements?
- Correlation between use of information elements and quality of the incident reports?
- Subjective experiences?
- Any training effects?

Results – quantitative use of elements

- Background
- Victim
- Attacker
- Incident description
- Damage Asessment



Results – qualitative use of elements



Correlation

- Small, but statistically significant, correlation r = 0.22 and p = 0.003 between the number of elements used and the quality.

Subjective ratings

- Content rating of 4.3 (scale 1-7).

- Too much information despite the efforts to create a simple template with only 16 information elements.

Conclusions

Overall

5 categories

Elements

Dynamics

Training

Log analysts