Beyond Incident Reporting

An Analysis of Structured Representations for Incident Response


Daniel Schlette (University of Regensburg, Germany)


Marco Caselli (Siemens AG, Germany)

About us.

Daniel Schlette

- PhD Candidate
- Faculty of Informatics and Data Science
- Cyber Threat Intelligence (CTI) and incident response

Marco Caselli

- Senior Key Expert
- Siemens research department “Cybersecurity & Trust”
- OT attack detection and response

SIEMENS

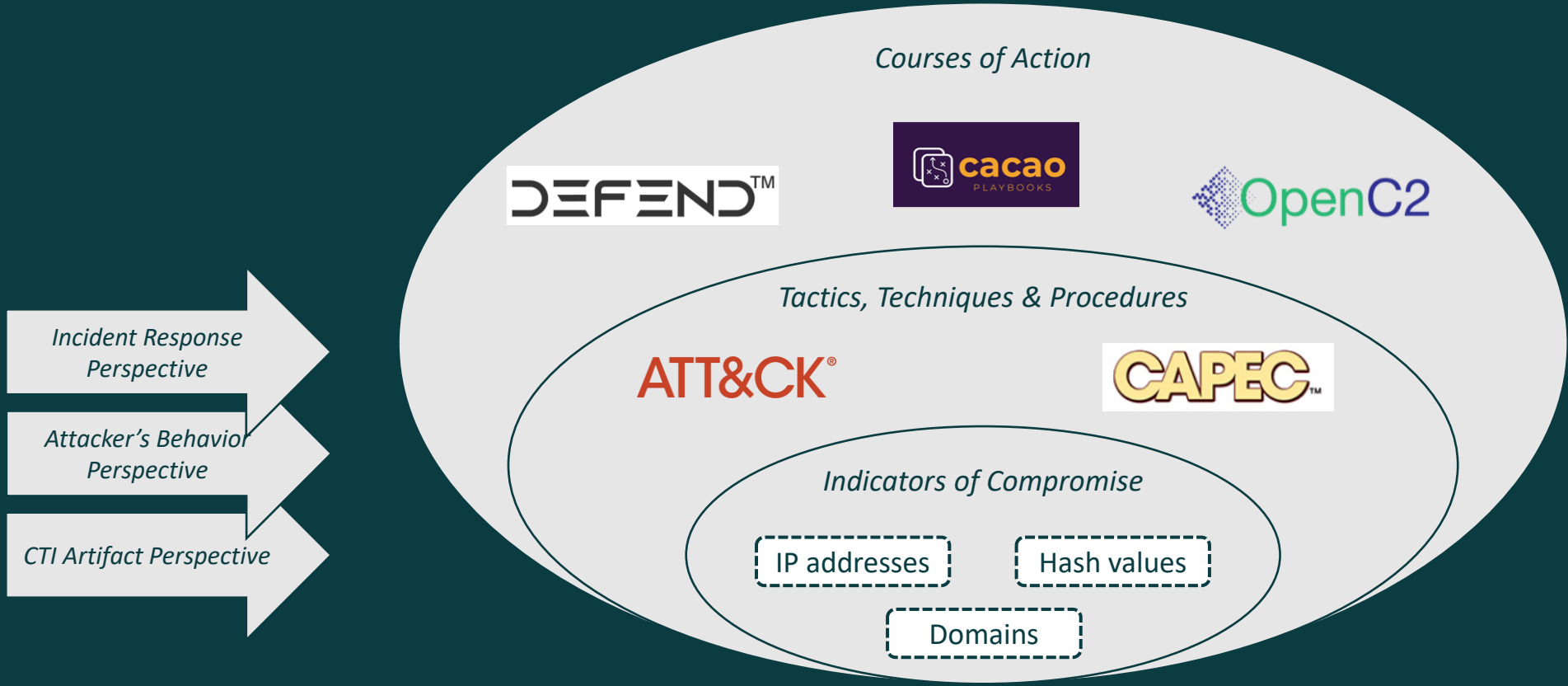
This talk can serve your organization to …

… have a look at incident response standards and formats

… compare and select these standards and formats using core concepts

… consider organizational factors for playbook modification

We observe a shift in perspective towards incident response representation.



Our motivations refer to the Neart Le Chéile theme.

General Context

- *US Executive Order 14028* is calling for standardized governmental playbooks
- *EU Cybersecurity Act* is addressing security teams and information exchange

Company Context

- CONCORDIA* and the ECCC
- Siemens Use Cases
  - ✓ *Incident response automation*
  - ✓ *Playbook sharing across teams*
  - ✓ *Internal reporting*

**https://www.concordia-h2020.eu/*

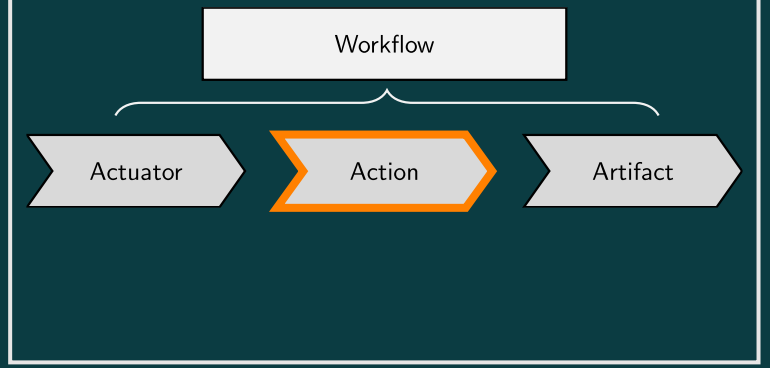
Identified challenges concern representation and operations.

- Incident Response Representation
  - ✓*How do we approach the problem?*
  - ✓*Which representation (e.g., standard) should we use?*
- Incident Response Operations
  - ✓*How do we integrate a representation in our pipeline?*
  - ✓*How do we ensure maintainability?*

Standardization efforts have different objectives that support categorization.

Incident response is defined by actuators, their actions, and artifacts.

Structural Concepts



Examples

- Analyst investigate file
- Security system block IP address
- Incident handler write report

We base our analysis on core concepts of incident response.

Structural Concepts	General Concepts	Technology Concepts	Security Concepts
Workflow	Aggregability	Community	Confidentiality
Actuator	Versioning	Application	Authorization
Action	Readability	Serialization	Prioritization
Artifact	Unambiguity		
	...		

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, 23(4), pp. 2525-2556.

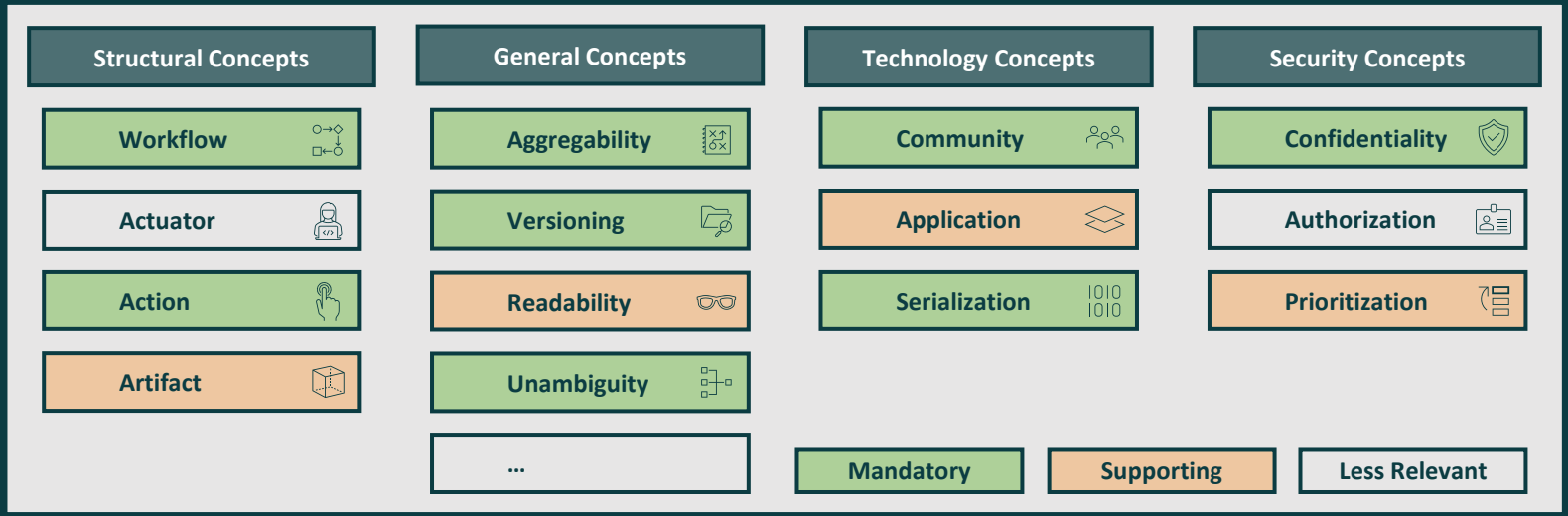
Characteristics of CACAO cover the core concepts (to some extent).

Structural Concepts	General Concepts	Technology Concepts	Security Concepts
Workflow steps	Playbooks	OASIS (technical)	TLP, FIRST IEP
Targets	Metadata	Direct, processes	Impact, owner
Commands	Machine	JSON	Priority, severity
(Variables)	(Definitions)		
	…		

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, 23(4), pp. 2525-2556.

Which format should you use for incident response sharing?

1. Define Use Case → 2. Rank Core Concepts → 3. Assess Formats

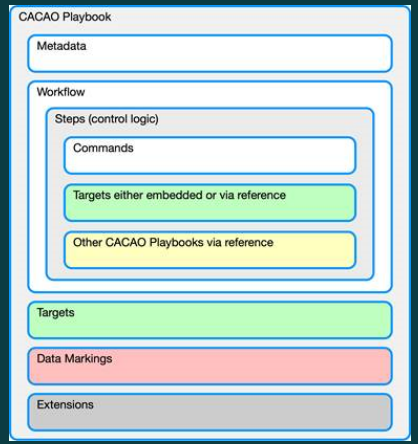


CACAO is a suitable candidate for incident response sharing.

Characteristics

- Playbooks aggregate information
- Procedures are represented by workflows
- CACAO is backed by the OASIS community
- TLP and IEP address confidentiality

Structure



The elephant in the room or why context matters.

CONTEXT MATTERS

Playbooks contain different types of information relevant for incident response operations.

Is organization-specific information important?

What determines organization-specific information?

We assume incident response is shaped by organization-specific factors.

Privacy

e.g., EU GDPR

Responsibility

e.g., chain of command

People

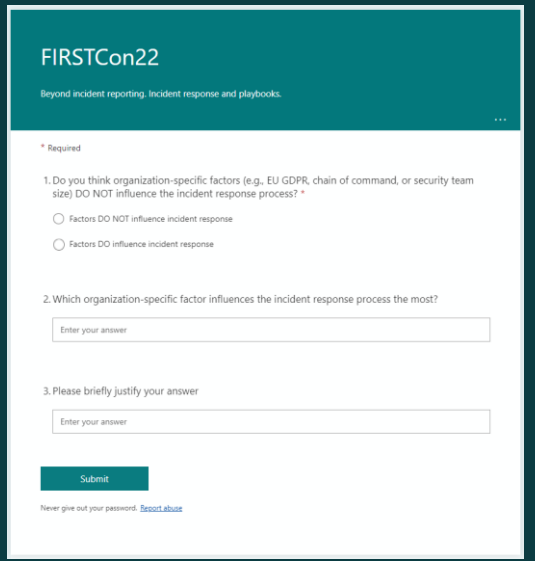
e.g., security team size

Do you think these factors do not influence the incident response process?

Do you think these factors do not influence the incident response process?

1. Scan QR code → **2. Enter your answer** → **3. Submit**

https://forms.office.com/r/d4XR4Uhk0b



Factors can modify the incident response process.

Baseline incident response process (simplified)

Baseline incident response process (simplified)

Factors can modify the incident response process.

Baseline incident response process (simplified)

Case 1: Privacy (GDPR applies)

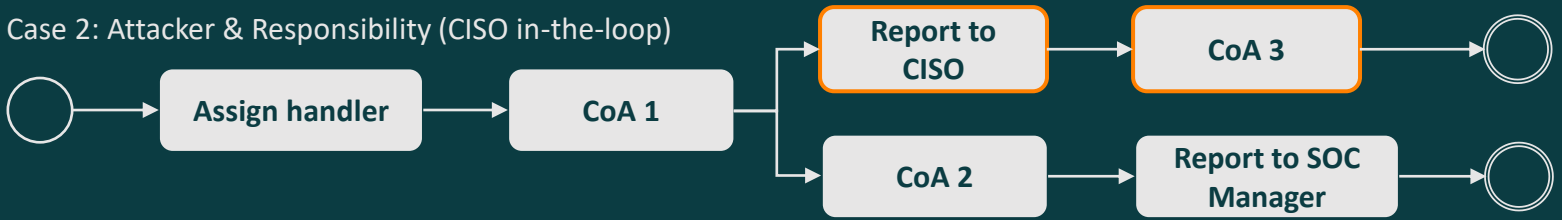
Baseline incident response process (simplified)

Factors can modify the incident response process.

Baseline incident response process (simplified)

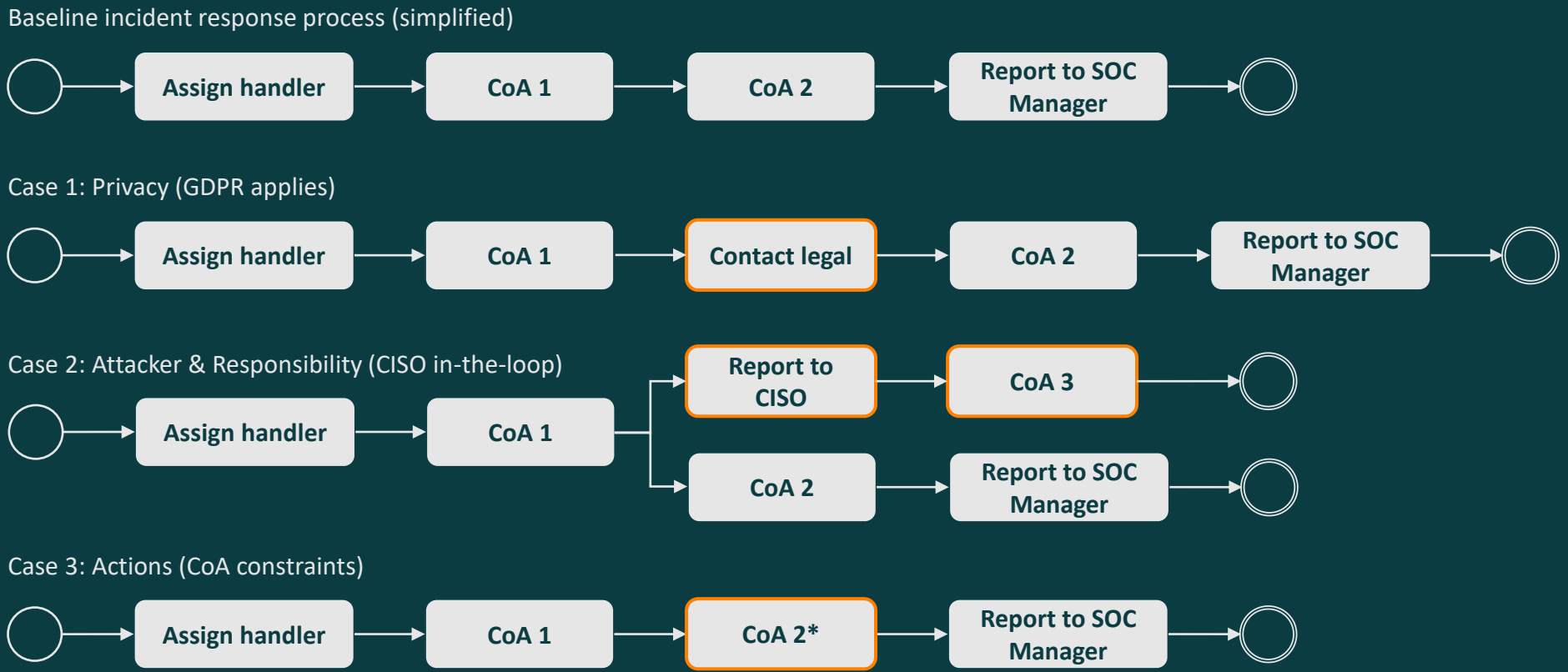
Case 1: Privacy (GDPR applies)

Case 2: Attacker & Responsibility (CISO in-the-loop)

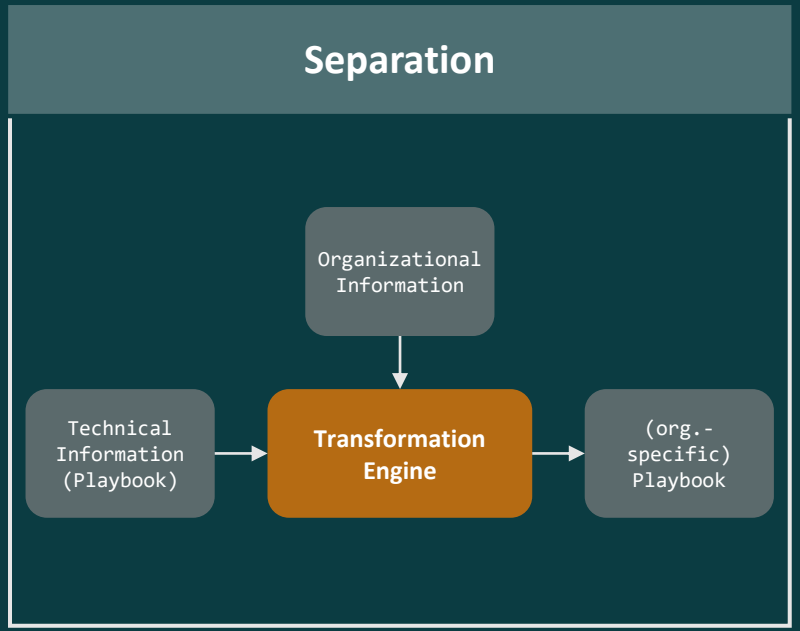


Baseline incident response process (simplified)

Factors can modify the incident response process.



Eventually, incident response factors can be used to separate playbook information.



Benefits

- Sharing playbooks without disclosing confidential information
- Adapting and (semi-)automating external playbooks
- Maintaining organizational information and playbooks when changes occur

Proposing incident response factors is an on-going project.

We conduct expert interviews to shed light on incident response factors.

Preliminary Feedback

- Interviewees mention modifications when factors apply
- Not all factors might impact incident response, but many do
- Additional feedback needed!

Thank you for your attention!

Contact Details

- Daniel Schlette
  daniel.schlette@ur.de
  linkedin.com/in/daniel-schlette

- Marco Caselli
  marco.caselli@siemens.com
  linkedin.com/in/marco-caselli

- IEEE Communications Surveys & Tutorials paper

Questions?