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
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.

- **Frameworks**
- **Playbooks**
- **Commands**

**Representation**

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

### Structural Concepts

- **Actuator**
- **Action**
- **Artifact**

### Examples

- Analyst investigate file
- Security system block IP address
- Incident handler write report
We base our analysis on core concepts of incident response.

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

Which format should you use for incident response sharing?

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

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Workflow</td>
<td>Aggregability</td>
<td>Community</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Actuator</td>
<td>Versioning</td>
<td>Application</td>
<td>Authorization</td>
</tr>
<tr>
<td>Action</td>
<td>Readability</td>
<td>Serialization</td>
<td>Prioritization</td>
</tr>
<tr>
<td>Artifact</td>
<td>Unambiguity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Mandatory
- Supporting
- Less Relevant
CACA0 is a suitable candidate for incident response sharing.

**Characteristics**

- Playbooks aggregate information
- Procedures are represented by workflows
- CACA0 is backed by the OASIS community
- TLP and IEP address confidentiality
The elephant in the room or why context matters.
Playbooks contain different types of information relevant for incident response operations.

- Organizational information
  - Ransomware expert: Jane Doe

- Technical information
  - `iptables -A INPUT -s 192.168.1.1 -j DROP`

Is organization-specific information important?

What determines organization-specific information?
We assume incident response is shaped by organization-specific factors.

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Responsibility</th>
<th>People</th>
</tr>
</thead>
<tbody>
<tr>
<td>e.g., EU GDPR</td>
<td>e.g., chain of command</td>
<td>e.g., security team size</td>
</tr>
</tbody>
</table>

Do you think these factors **do not** influence the incident response process?
Do you think these factors **do not** influence the incident response process?
Factors can modify the incident response process.

Baseline incident response process (simplified)

Assign handler → CoA 1 → CoA 2 → Report to SOC Manager

Baseline incident response process (simplified)

Assign handler → CoA 1 → CoA 2 → Report to SOC Manager
Factors can modify the incident response process.

Baseline incident response process (simplified)

- Assign handler
- CoA 1
- CoA 2
- Report to SOC Manager

Case 1: Privacy (GDPR applies)

- Assign handler
- CoA 1
- Contact legal
- CoA 2
- Report to SOC Manager

Baseline incident response process (simplified)

- Assign handler
- CoA 1
- CoA 2
- Report to SOC Manager
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.

Baseline incident response process (simplified)

Case 1: Privacy (GDPR applies)

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

Case 3: Actions (CoA constraints)
Eventually, incident response factors can be used to separate playbook information.

**Separation**

- **Technical Information (Playbook)**
- **Transformation Engine**
- **Organizational Information**
- **(org.-specific) Playbook**

**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