Mohamed Trigui
Zuha Ansari
Group 11
9/23/2025

Research Paper Summary

1. Title and Citation of the Paper:

- **Title:** Model-Based Incident Response Playbooks
- **Authors:** Avi Shaked, Yulia Cherdantseva, Pete Burnap
- **Year of Publication:** 2022
- **Full Citation (in the preferred citation style):**
  Shaked, A., Cherdantseva, Y., & Burnap, P. (2022, August 23–26). Model-based incident response playbooks. *Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES 2022) (pp. 1–7)*. Association for Computing Machinery. https://doi.org/10.1145/3538969.3538976

2. Objective and Research Question:

- **What is the main objective of the paper?**
- **What research question(s) does the paper aim to address?**

The main goal of this paper is to show that incident response playbooks can be represented in a more formal and structured way instead of being just text documents or simple diagrams. The authors wanted to answer whether it is possible to design a metamodel that can represent playbooks consistently, and whether a tool based on that metamodel can help people design and share playbooks more effectively. We feel like their main question was: Can incident response playbooks be modeled in a machine-readable, process-oriented way that supports coordination and learning?

3. Technique/Methodology:

- **What technique or methodology is proposed or used in the paper?**
- **How does this technique contribute to the field? Is it a novel approach or an improvement over existing methods?**

This is a design-based research paper. The authors identified seven key concepts of IR playbooks (such as tasks, resources, references, roles, etc.) and used them to develop a metamodel. They then built a prototype tool in Java on Eclipse (Github repo: https://github.com/CardiffUniCOMSC/SecMoF), using its modeling framework and the

PROVE tool as a base. They extended PROVE to handle IR-specific concepts, calling their new version FRIPP (Formalized Response to Incidents Process Playbook).

We see this as a contribution because it moves IR playbooks from being descriptive and inconsistent into a formalized and machine-readable format. Compared to existing approaches like CACAO or RE&CT, FRIPP provides a stronger foundation and allows gaps and inconsistencies in playbooks to be visualized. It is not an entirely new concept to model processes but applying it specifically to IR playbooks in this structured way is what makes it valuable.

4. Dataset(s) Used:

- **What dataset(s) were used for experimentation and analysis?**
- **Are these datasets publicly available, and do they represent the problem space adequately?**

There were no experimental datasets in this study. Instead, the authors tested their prototype using well-known, publicly available frameworks such as Integrated Adaptive Cyber Defense (IACD), NIST guidance, and OASIS CACAO. These frameworks already provide structured examples of playbooks that cover different IR stages (planning, mid-incident, post-incident). The authors modeled these frameworks in their tool to demonstrate that FRIPP can capture their logic. So while there was no "dataset" in the typical sense, they worked with recognized playbook libraries that the security community relies on.

5. Empirical Results:

- **What experiments were conducted to validate the technique?**
- **What were the key metrics used to evaluate performance (e.g., accuracy, precision, recall, F1-score)?**
- **Summarize the empirical results and how they compare to baseline methods or previous work.**

Since this was design-based research, there were no quantitative results like accuracy or F1-scores. Instead, the validation came from showing that the FRIPP prototype could model existing playbooks and visually display their structure. The prototype also produced interactive graphics. These graphics clearly showed connected processes and highlighted any missing parts by using red question marks or empty brackets. They also introduced a "Related References" container that connects the modeled steps back to the original written protocols. This was a way to give analysts more context while still

keeping the playbook visual and structured. Overall, the results demonstrate feasibility rather than performance.

6. Overall Results and Findings:

- **What are the main findings of the paper?**
- **How do the results support or refute the initial hypothesis or research question?**
- **Did the authors discuss any limitations or future work?**

The main finding is that IR playbooks can indeed be formalized in a model-based way, and doing this makes them easier to read, share, and analyze. The FRIPP prototype not only represented playbooks consistently but also exposed gaps in their design, something that is very hard to see in plain text.

The authors are clear that this is just the beginning. They plan to extend their metamodel with more domain knowledge, work with practitioners to refine the playbooks, and eventually include things like timestamps of actions to measure efficiency. They also mention that they want to explore "enacted IR processes" so that the model doesn't just describe what should happen, but also tracks what did happen during a live incident. This would push their model toward being more integrated with the IR lifecycle.

7. Student's Insights and Critical Analysis:

- **What are your insights or reflections on the paper?**
- **Do you find the methodology and results convincing? Why or why not?**
- **How could this work be improved or extended in future research?**
- **How does this paper contribute to your own research or the field in general?**

We think this paper is a solid foundation for anyone who wants to take IR playbooks seriously. It makes sense to formalize them before we talk about automation or advanced analytics. The way they used FRIPP to show gaps with red marks is very practical, because it immediately shows an analyst where their playbook might be incomplete.

At the same time, the work feels a bit limited. The evaluation only used examples from frameworks, and we feel it would have been stronger if they tested it with real-world SOC playbooks. Also, the tool is more about design than about automation. It does not actually run or execute the playbooks. For us, that's the big opportunity: once playbooks are formalized, the next logical step is to connect them to execution engines and ATT&CK mappings so that the playbooks become actionable.

If we were to extend this paper, we would definitely add ATT&CK technique IDs to each task. That way the playbook is tied directly to adversary behavior. We would also provide a BPMN export option because BPMN is already a global standard for workflows, and many SOC tools could benefit from it. Finally, creating an engine that reads the playbook and actually runs the steps (with human approval in the loop) would be a huge leap forward.

8. Relevance to Your Research:

- **How is this paper relevant to your current research focus or thesis?**
- **Can any of the techniques or findings be applied or adapted to your research?**

This paper is highly relevant to what we are working on. Our research is about mapping IR playbooks to MITRE ATT&CK using BPMN. The baseline paper gives us the modeling foundation: it proves that playbooks can be structured in a formal way. But it doesn't connect playbooks to ATT&CK and it doesn't go into execution.

In our work, we plan to take BPMN playbooks and tag each task with ATT&CK technique IDs. This means that when a SOC analyst runs the playbook, they can clearly see which adversary behavior the step is addressing. We also want to go further and see how BPMN playbooks can be executed automatically, for example by connecting them to security tools or SOAR platforms.

So while the baseline paper focuses on how to model playbooks, our contribution will focus on how to operationalize them. We think the two complement each other well. Their work gives us the "language" of playbooks, and we are building the bridge to ATT&CK and automation so that the models can have a direct impact in practice.