EuroVis Workshop on Visual Analytics (2024)
M. El-Assady and H.-J. Schulz (Editors)

Visually Supporting the Assessment of the Incident Management Process

Alessandro Palma[1] and Marco Angelini[1,2]

[1]Sapienza University of Rome, Rome, Italy
[2]Link Campus University, Rome, Italy

Abstract

Incident Management (IM) is the process to prevent, protect, and react to incidents affecting an organization and should be well-defined to be prepared in case of alerts. To this aim, security standards define guidelines to manage the incidents and the organizations should comply with them to properly set up a secure-by-design process. Assessing whether an organization is compliant or not with security standards requires a big effort as the main methodologies are based on manual analysis and leveraging automatic approaches to support human decisions is challenging. To facilitate this task, we design IMPAVID, a visual analytics solution to support the assessment of IM process compliance through process mining. The aim is to increase the level of awareness of the security assessor to support her in making informed decisions about actions to improve IM process compliance with regulatory and technical standards. We evaluate the proposed system through a usage scenario based on a publicly available dataset containing data from a real IM log of an IT company.

CCS Concepts

• ***Human-centered computing*** → ***Visual analytics; Visualization systems and tools;*** • ***Security and privacy*** → *Usability in security and privacy;*

1. Introduction

According to ISO 27035 [ISO13], *Incident Management* (IM) is the process of detecting, reporting, assessing, responding to, dealing with, and learning from security incidents. Nowadays, it is common for a company to be involved in different incidents [AHR12], which may impact its business, reputation, and security. Therefore, it is crucial to be prepared to timely react and contain incident consequences. If not properly managed, IM requires a big effort to organize the security procedures and handle the incidents. Many security standards exist to support organizations during IM, such as ENISA [Eni23], ISO 27035 [ISO13], and COBIT [IT 19]. They describe the main phases of performing the IM process, and the goal of the organizations is to be compliant as much as possible with such standards to prevent unwanted consequences.

To evaluate compliance, a human assessor compares the actual process performed by the organization with a reference one provided by a standard: this activity is usually labeled as *process compliance assessment* [dLM17]. The first challenge of performing this task is due to the lack of standard metrics to measure compliance with standards, hindering objective decisions and analyses. Moreover, most of the standards are intentionally general and potentially lead to different interpretations: this makes it hard to measure how effective and accurate are human decisions. A final emerging problem is that IM process compliance is typically performed through interviews and manual analysis of the collected information, that are mapped to the indications provided by the reference process model. This implies that human errors and bias are always possible in each step of the assessment, as well as different sensibilities from different assessors to similar situations that may influence the evaluation, beyond the fact they are typically time and resource-consuming [MCB*17, FHBM12].

To mitigate these problems, we propose IMPAVID (Incident Management Process Assessment through Visual Interactive Data analysis), a visual analytics solution to support process compliance assessment during IM. It leverages process mining [vdA16] to identify the deviations of an IM process to the reference one. Differently from the current literature, this enables the analysis to consider both compliance and technical aspects of the incidents, allowing hypothesizing interventions that raise the compliance of the IM process with a reference standard. This paper contributes the following:

- a collection of analytical requirements extracted from security standards that informs the design of the proposed solution;
- the design and implementation of IMPAVID for the assessment of IM process compliance with a reference model;
- the development of a usage scenario on a real dataset showing the capabilities of IMPAVID during process compliance assessment.

2. Background and Related Work

Process compliance assessment is the evaluation of the compliance of a process implemented by an organization with a reference one. It is based on a *process log* and a *reference process model*. In the case of Incident Management (IM), the former collects information about the lifecycle of the incidents, which is the set of sequential activities performed to manage the incidents. For each incident, it includes its identifier, the activities performed with their timestamps, technical features (e.g., impact,

DOI: 10.2312/eurova.20241116

category), and the actors who detected, opened, resolved, and closed the incident [AS12]. Typically, organizations use ticketing systems to automatically collect this information (e.g., [Ser16]). The latter is the representation of the IM process described by a security standard (e.g., ISO 27035 [ISO13]) in Business Process Modeling (BPM) format (e.g., Petri Net [Pet66]). It is easily obtainable through user-friendly modeling tools (e.g., WoPeD [EF08]). The state-of-the-art in process mining leverages *trace alignment* [ASv11, dLM17] to automatically detect the deviations of a process log from the reference process model. It indicates for each trace (i.e., incident in the case of IM), the set of activities non-compliant with the reference model, namely *process deviations*. In this paper, we propose a Visual Analytics (VA) solution to support the IM process compliance assessment by introducing an analytical model that leverages trace alignment to calculate the *non-compliance cost*.

Considering VA solutions in the IM domain, many works address technical aspects of the incidents, focusing on the response phase [APS15, NG09, KKG20] and attack tracking [dABM*18, FPB*17]. Other ones put the attention on the IM as a process, as Gove [Gov21], who designs a narrative visualization for incident reports to give analysts a succinct view of the information contained in an incident report. Similarly, Novikova et al. [NBS17] present a set of VA techniques to monitor information security and event management, including incidents, while Cavalcante et al. [CPS*12] propose an analytical tool to characterize the performance and quality of time-bounded IM systems. While these works are focused on technical aspects of the incidents, our solution analyzes in-depth the process itself, its compliance with standards, and the relations between incidents. To this aim, a promising solution to address this problem is the combination of VA with process mining [vdAdLtH11, Mik21]. Among the works leveraging this combination, Rasmussen et al. [RER*10] investigate two approaches to improve analyst performance on monitoring tasks by correlating Intrusion Detection System data and defensible recommendations based on learning from historical data. Differently, Knuplesch et al. [KRK17] present a comprehensive framework for visually monitoring business process compliance under the perspective of time, control flow, resources, and data. Duan et al. [DZSC18] present an approach for checking security properties and compliance to represent complex logic formulas through a visual compliance rule modeling language. Finally, Angelini et al. [ALS17] propose a VA solution to support security managers during the assessment based on the NIST cybersecurity framework [NIS21]. Let us note that all these works consider compliance with specific requirement rules, checking whether they are satisfied or not. In contrast, they do not provide support to a security assessor during the process compliance, as we propose in this paper, through a comprehensive analysis integrating both technical and compliance aspects of the IM.

3. Requirements collection

In this section, we detail the requirements that are necessary to assess the IM process. To inform the system design, we first surveyed the state-of-the-art and collected requirements. We reviewed IM security standards, which are COBIT CMM (Capability Maturity Model) [Ins07], ISO 27035 [ISO13], and ENISA [Eni23]. The assessment requirements collection has been performed jointly with two security experts who read the standards and extracted all the information about the IM process compliance assessment. Then, they organized this information into analytical tasks, identifying four macro objectives according to COBIT CMM. A third security expert involved in auditing activities supervised the requirement collection, projecting the human workflow perspective with her expertise through one specific session.

More in detail, the two security experts have practical experience in technical incidents and less in the IM process, while the third one was involved in a feedback session on the document analysis and process perspective. In the rest of this section, we describe the nine collected requirements organized into four objectives according to the process management lifecycle: prerequisites, process capability, quality control, and management information.

Prerequisites. As a first objective, the assessor must check whether the information used for the assessment is trustworthy and complete. She defines the goals of the assessment and the IM activities that must exist to be compliant with security standards. To do so, the assessor analyzes the percentage of the incidents under analysis and the available resources to guarantee that the amount of evidence is enough to perform the assessment.
RQ1 - The system must provide the overview of the analyzed incidents, their impact, and the reference model to comply.

Process Capability. The second objective involves causal analysis to assess what an IM process ought to include and what it is missing. The scope of this step is the analysis of the internal implementation of the process and goes into the detail of the executed IM (RQ2). To do so, the assessor analyzes how the process evolves and which are common IM executions (i.e., process patterns) adopted by the organization (RQ3), identifying some common behaviors.
RQ2 - The system must support the analysis of the IM evolution over time (temporal analysis);
RQ3 - The system must support the classification of the incidents based on the IM process execution.

Quality Control. The next objective is to check the process quality, measured through suitable metrics. To this aim, we leverage the *fitness* [ASv11, dLM17] that is a trace alignment metric, expressed with a value between 0 (no log activity matches with the target model) and 1 (all log activities match the model), and measures the overall number of deviations in the log. In combination with the fitness, we designed an analytical model (see Section 4.1) to measure the *non-compliance cost*, quantifying the impact of the problems affecting compliance (RQ4). Beyond these metrics, the assessor checks that all incidents are resolved and closed (RQ5) together with the common process patterns (RQ6).
RQ4 - The system must support the identification and analysis of the main causes of non-compliance;
RQ5 - The system must support the identification and analysis of resolved/closed incidents;
RQ6 - The system must support the identification and analysis of possible incident patterns.

Management Information. The last objective is the analysis of incident details, with a particular focus on critical non-compliant incidents (RQ7). The assessor highlights the weakest parts of the IM process in terms of compliance (RQ8) in comparison to the reference process (RQ9), focusing on single incidents when needed. This is a crucial aspect to support decisions aimed at improving the IM.
RQ7 - The system must support the identification and analysis of the details of the most critical deviations;
RQ8 - The system must support the identification and analysis of incidents impacting compliance the most;

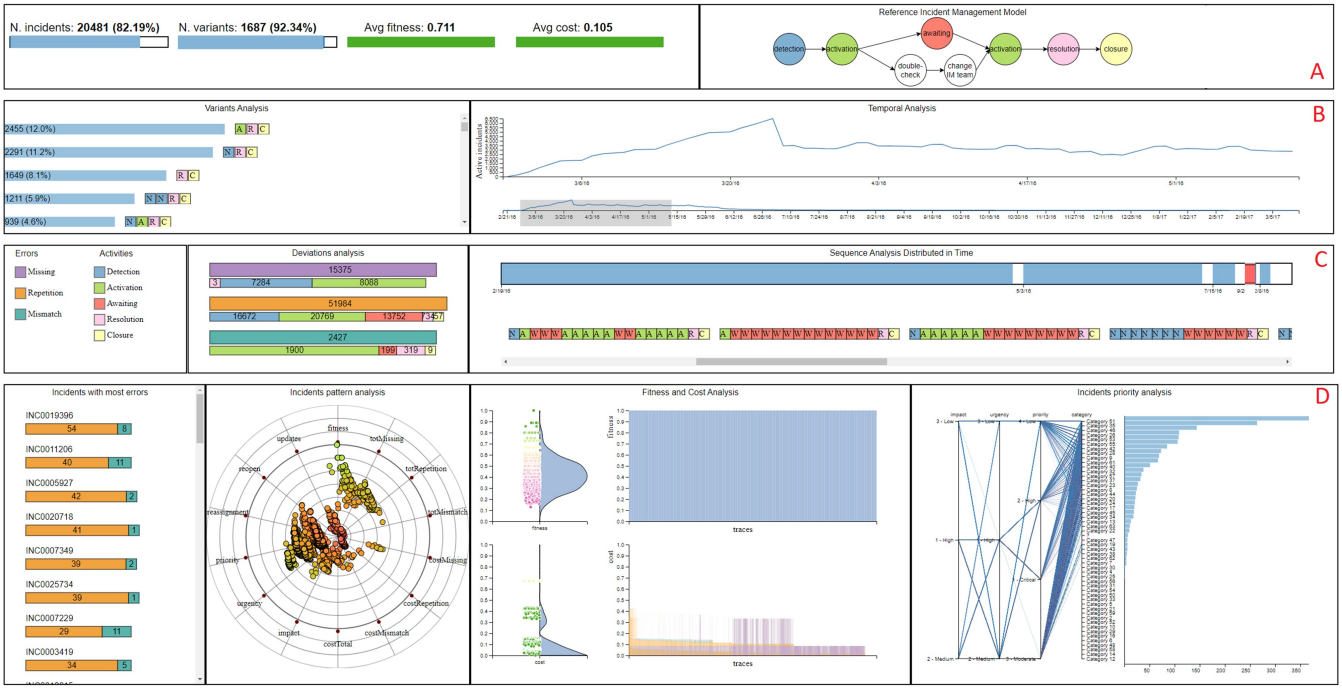

Figure 1: *Overview of the IMPAVID system.*

RQ9 - The system must support the exploration of the process quality in terms of fitness and cost metrics.

4. The IMPAVID system design

The IMPAVID system is developed using web technology and designed to support a security assessor during the IM process compliance assessment. In this section, we describe the visualization design that supports the collected requirements. The system is available at https://github.com/Ale96Pa/IMPAVID.

IMPAVID is composed of four horizontal panes, from top to bottom. Each one addresses one assessment objective according to analyzed IM standards, thus structurally guiding the user during the assessment. Thus, the analyst can analyze one pane at a time, or even different users analyze different panes (as typically happens in Security Operation Centers). This reduces the potential cognitive overload of analyzing all the panes together.

The *Overview Pane* (Fig. 1-A) reports the overview of the whole assessment, highlighting aggregated scores (i.e., the number of selected incidents and their variants, the average fitness and cost) for the most important metrics (e.g., percentage of incidents under analysis, amount of different trace variants). These metrics are accompanied by colored bars encoding how good they are (i.e., from green if the metric presents a good score to red if the score alerts the attention of the assessor), adaptable to a color-blind safe scale. In the right part of the pane, there is an interactive state diagram representing the reference process model, always visible during the assessment, showing the control flow of the expected IM activities. It can be zoomed in for large diagrams. The overview pane provides the overall compliance of the IM process under scrutiny (**RQ1**). We encoded each activity with a different color as well as each type of deviation (i.e., missing, repetition, and mismatch), while the light blue color was chosen for neutral elements (i.e., not requiring a specific encoding). When the number of activities is particularly conspicuous to assign one color for each, it is suitable to batch them and assign to the group a color (e.g., grouping by similar functionality). These colors are coherent within the whole system and visually coordinate the different visual representations of the same entities in the different panes.

The second pane is the *Execution-Analysis Pane* (Fig. 1-B). It allows to explore and study the most frequent IM processes and their composing activities. It reports the unique process executions (represented as a sequence of activities [RPC*00]) on the left, sorted by the number of times they occur. This view allows for exploring and identifying the most common process executions (sequences of activities) of the IM process. Given the importance of classifying the incidents based on their execution (**RQ3**), we use blue bars on the left to distribute the trace variants, followed by the sequence of activities of the corresponding execution with colors coherent with the reference process model view. On the right, the temporal analysis is represented through a line chart showing the distribution of active incidents (on the y-axis) over time (on the x-axis). This view uses the focus+context paradigm [Fur86, SA82], in which the whole distribution is always present in the lower part (context), while the upper part highlights only the selected period (focus) through horizontal brushing on the context. This supports the analysis of the IM evolution over time, identifying potential critical periods for

occurrences and recurring sequences of activities (**RQ2**).

The third pane is the *Deviation Pane* (Fig. 1-C). It supports the assessor in analyzing the deviations of the executed process from the reference one, using the analytical model (see Section 4.1). On the left, there is an interactive legend working as a filter for error categories (i.e., missing, repetition, and mismatch) and activities (e.g., detection, activation, awaiting, resolution, and closure). In the middle, a horizontal composite stacked bar chart represents how much each deviation is present (top bar) and its breakdown by composing activities. In this way, it provides a view of the main errors affecting the process (**RQ4**) and the distribution of the corresponding activities (**RQ5**). The incidents distribution view completes this pane on the right. The distribution is represented as a horizontal "tape" to allow a continuous scrolling view. It comprises single activities aggregated by incident trace, enabling the analysis of both the distribution and the sequence of incident executions (**RQ6**). Blue bars indicate the distribution of the incidents in five periods, equally sampled from the process history [RPC*00]. By clicking each bar, the sequence of incident executions sorted per time appears below.

The last pane is the *Incidents Pane* (Fig. 1-D), supporting the detailed analysis of the incidents. It is composed of four views that, from left to right, progressively increase the level of detail. The first one is a horizontal stacked bar chart of the occurred incidents, with deviation breakdowns, sorted by the number of deviations. Its goal is to prioritize intervention on incident traces presenting the highest number of deviations (**RQ7**). The second chart is a RadViz plot [ABL*21], representing the distribution of the incidents according to the IM log features, that analyzes the most influential features for identifying common patterns (**RQ8**). These features are not part of the process compliance analysis but are technical features of each incident (e.g., impact, priority, etc.). Its goal is to allow analysis of incident similarity for groups of incidents with similar deviation distribution. The third visualization is a combination of a violin plot [HN98] and a bar chart for fitness and non-compliance cost metrics. The violin plots give two different insights: on the left, the spread of incidents related to the fitness (on top) and cost (on bottom) metrics (**RQ9**), and on the right, their current distribution by error type (**RQ7**). The bar chart of the cost reports the impact of each error category on the total cost of each incident, providing fine-grained information on the most impactful deviations. The last chart is a combination of parallel coordinates [ID91] and a bar chart. The parallel coordinates are highlighted in red to show the categorical features of the selected incidents, while the bar chart shows the distribution of the different types of incidents. The points in radviz and violin plots have the same color encoding representing the non-compliance cost as in the first pane (i.e., from green, meaning a good score, to red meaning a bad one). All the views are interactive to filter the analysis for specific incidents by brushing axes or selecting elements.

4.1. Dynamic Deviation Cost Analytical Model

We assess the non-compliance cost of the IM process with an analytical model based on process deviations designed as follows [AAB*22]:

Step 1. We define three error categories to distinguish the different causes of non-compliance. They are: (i) *missing activities*, i.e., errors in which some necessary activities are missing in the log (e.g., missing detection due to hidden attack); (ii) *repeated activities*, i.e., errors due to the repetition of the same activity more than once in the log (e.g., multiple resolutions due to complex management); (iii) *mismatching order*, i.e., errors due to the wrong sequence of activities execution (e.g., closing an incident before opening it). The rationale for these definitions is to capture all possible deviations that may arise during an IM process [AAB*22].

Step 2. The second step consists of assigning weights to each deviated activity to represent the penalty it provides to the IM. For example, an assessor may know that *missing detection* could be a deviation due to a cyber attack the analyst cannot detect (e.g., hijacking or man-in-the-middle attacks). S/he can determine such deviation as much more severe than *missing closure*, which may indicate that the service desk just forgot to flag the incident as closed. More formally, we will use the following notation: the reference model is composed of a combination of N different events (i.e., the number of different IM process activities) $E_1,...,E_N$, while I denotes an incident in the log, composed by a combination of $E_1,...,E_N$, with $|I|$ being the number of activities in I. Let $H(E_i)$ be equal to 1 if the activity E_i is missing in I and 0 otherwise, let r_{Ei} and m_{Ei} be the number of times the activity E_i is consecutively repeated and mismatched respectively. Then, the non-compliance cost of an incident I for each error category is:

$$\begin{cases} miss(I) = \sum_{i=1}^{N} \alpha_i \cdot H(E_i) \\ rep(I) = \sum_{i=1}^{N} \beta_i \cdot \frac{r_{Ei}}{|I|} \\ mismatch(I) = \sum_{i=1}^{N} \gamma_i \cdot \frac{m_{Ei}}{|I|} \end{cases} \quad (1)$$

where α_i, β_i, and γ_i are parameters to weight missing, repetition, and mismatch errors respectively, for each activity E_i. The assessor can dynamically change this parameterization to try different hypotheses for deviation costs and compare multiple runs, looking for the most fitting

Step 3. Once each incident has associated a non-compliance cost for each of the missing, repetition, and mismatch deviations, the last step combines them to determine the incident non-compliance cost. We use a linear combination of the errors' cost resulting in:

$$cost_{NC}(I) = w_m \cdot miss(I) + w_r \cdot rep(I) + w_s \cdot mismatch(I), \quad (2)$$

where w_m,w_r, and w_s are weights for missing, repetition, and mismatch errors respectively. Notice that the assessment model is parametric in the error weights, and the assessor must manually assign different severity levels depending on the context and her expertise. While the error categories are encoded in all the panes and explicitly listed in the filter selection of the Deviation pane, the assessor can examine the cost of non-compliance in the Overview pane for assessing the overall status, and in the Incident pane for analyzing the cost of individual incidents.

5. Usage Scenario

To show the capabilities of IMPAVID to support security assessors, we provide a usage scenario of an IM process compliance assessment with ISO 27035 standard [ISO13] using a publicly available log including real data of an IM process from the audit system of the ServiceNow™ [Ser16] platform used by an IT company [AFRP19]. It contains 141,712 events organized in 24,918 incidents and for each event, 32 descriptive attributes there exist related to the incident process (i.e., number of updates during the incidents), classification (i.e., categories of the incident), and diagnosis (i.e., impacts).

Step 1. Starting from the overview (Fig. 2-step 1), the assessor sees that she loaded the full log (24,918 incidents), which has an average fitness of 0.719 and non-compliance cost equal to 0.102. This informs the assessor that the IM process is not fully compliant with ISO 27035, although the situation does not seem necessarily critical at this stage.

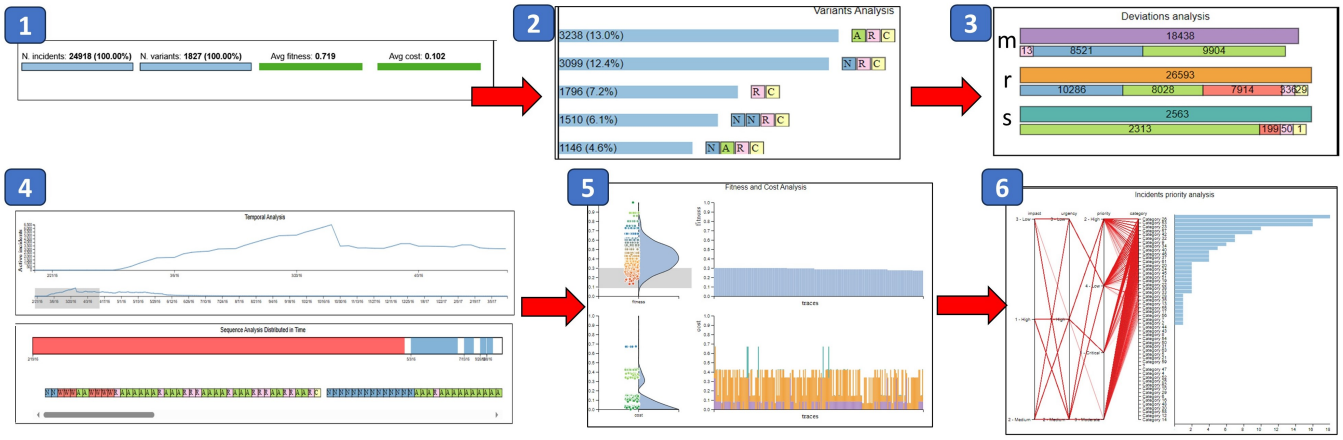

Figure 2: *Illustration of the usage scenario demonstrating a workflow of IM process assessment.*

The assessor spots that there are 1827 different ways in which incidents have been managed by the organization. This means that on average 7.2% of the incidents have the same process execution, communicating too high heterogeneity and the presence of multiple deviations.

Step 2. The assessor analyzes the most frequent process variants in detail (Fig. 2-step 2). She discovers that the most frequent traces are non-compliant with ISO 27035: 13% (3238) of the incidents missed the detection phase, 12.4% (3099) missed the activation phase, and 7.2% (1796) missed both of them. The assessor selects them to continue the analysis. This means the organization tends to fail at the initial steps of the IM, therefore consequences can be propagated in the process.

Step 3. To further investigate the causes for non-compliance, the assessor shifts to the Deviation analysis (Fig. 2-step 3), which reports that 18,438 activities are missing (*m*), 26,593 are repeated more than needed (*r*), and 2563 are mismatched (*s*). In all cases, most of the problems are caused by the detection (blue bars) and activation (green bars) activities, which are confirmed to be the most critical parts of the process.

Step 4. At this point, it is necessary to study how the process evolves over time to study the propagation of the identified problems. The assessor focuses on the Temporal Analysis (Fig. 2-step 4, top) showing the trend of active incidents during time. From the line chart, the first period was affected by thousands of incidents reaching peaks of 6500 incidents per day. In the last part, the incidents are less than hundreds per day. This means that either the organization improved its process or that the last period was less critical for the IT applications. Thus, the assessor selects the incidents that happened in the first 90 days to interpret the peak of the temporal analysis: looking at the Sequence analysis (Fig. 2-step 4, bottom), she discovers that the number of activities needed for the IM process was increasing over time. This explains the reasons for the initial peak, which is due to the bad management of the first incidents, causing a delay in the next ones.

Step 5. To further analyze the problematic incidents, the assessor selects the lowest fitness values from the violin plot on top (Fig. 2-step 5) to analyze the less compliant incident processes. From the corresponding analysis of the non-compliance cost (Fig. 2-step 5, bottom), she discovers that the errors due to missing activities are rarely very costly, but they affect most of the traces with a mean cost of 0.1; the repetition error occupies a greater part of the bar chart with an average cost of 0.4, resulting in a moderately costly error; finally, the mismatching errors are rare but very costly, reaching peaks of 0.7 in the most critical incidents. Selecting the incidents with the highest cost, the assessor identifies 102 incidents, which cumulatively weigh the most for the non-compliance cost. She identifies a sub-group of process traces that mostly affect non-compliance, passing from 24,704 to analyze due to the fitness metric to 102, and a second sub-group to analyze later (moderate cost, 478 traces).

Step 6. Thanks to this reduced number, the assessor can conclude the analysis by studying the types of incidents that significantly affect the process compliance to check for root causes in the type of incidents (e.g., phishing, DDoS) and their impact (Fig. 2-step 6). Since the log contains real data, it is anonymized for privacy issues, and it reports category IDs referred to incident types. For example, Category 26 in Fig. 2-step 6 may correspond to incidents caused by phishing attacks (which are the most common ones). A possible mitigation action would be investing more resources to train employees in recognizing phishing decoys (e.g., fake emails). With the mitigation applied, the assessor observes a reduction of the non-compliance cost from 0.102 to 0.065 and can repeat the analysis (eventually with different filters) to further enhance compliance.

6. Conclusions

This paper presented IMPAVID, a VA solution that supports security assessors during IM process compliance. It integrates an analytical model to measure the non-compliance cost that prioritizes the most critical non-compliant incidents. The visualization design has been informed and led by the collection of nine requirements from security standards and a usage scenario demonstrates the capabilities of the system to guide the assessor to make informed decisions about process compliance. Current limitations are the missing exploration of the parameters of the analytical models, which we plan to address through a parallel visual interface, the involvement of stakeholders in conducting a user study, and the implementation of guidance means to reduce the cognitive workload.

Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

References

[AAB*22] ACITELLI G., ANGELINI M., BONOMI S., MAGGI F. M., MARRELLA A., PALMA A.: Context-aware trace alignment with automated planning. In *2022 4th International Conference on Process Mining (ICPM)* (2022), pp. 104–111. doi:10.1109/ICPM57379.2022.9980649. 4

[ABL*21] ANGELINI M., BLASILLI G., LENTI S., PALLESCHI A., SANTUCCI G.: Effectiveness error: Measuring and improving radviz visual effectiveness. *IEEE Transactions on Visualization and Computer Graphics* (2021), 1–1. doi:10.1109/TVCG.2021.3104879. 4

[AFRP19] AMARAL C. A. L., FANTINATO M., REIJERS H. A., PERES S. M.: Enhancing completion time prediction through attribute selection. In *Information Technology for Management: Emerging Research and Applications* (2019), Springer International Publishing, pp. 3–23. doi:10.1007/978-3-030-15154-6_1. 4

[AHR12] AHMAD A., HADGKISS J., RUIGHAVER A.: Incident response teams – challenges in supporting the organisational security function. *Computers & Security 31*, 5 (2012), 643–652. doi:https://doi.org/10.1016/j.cose.2012.04.001. 1

[ALS17] ANGELINI M., LENTI S., SANTUCCI G.: Crumbs: A cyber security framework browser. In *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)* (2017), pp. 1–8. doi:10.1109/VIZSEC.2017.8062194. 2

[APS15] ANGELINI M., PRIGENT N., SANTUCCI G.: PERCIVAL: proactive and reactive attack and response assessment for cyber incidents using visual analytics. In *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)* (Oct. 2015), pp. 1–8. doi:10.1109/VIZSEC.2015.7312764. 2

[AS12] ACCORSI R., STOCKER T.: On the exploitation of process mining for security audits: the conformance checking case. In *Proceedings of the 27th Annual ACM Symposium on Applied Computing* (2012), pp. 1709–1716. doi:10.1145/2245276.2232051. 2

[ASv11] ADRIANSYAH A., SIDOROVA N., VAN DONGEN B. F.: Cost-based fitness in conformance checking. In *Int. Conf. on Application of Concurrency to System Design* (2011), IEEE, pp. 57–66. doi:10.1109/ACSD.2011.19. 2

[CPS*12] CAVALCANTE V., PINHANEZ C. S., SOUZA C. B. D., PAULA R. A. D., APPEL A. P., ANDRADE C. S.: Characterizing Time-Bounded Incident Management Systems. In *2012 Annual SRII Global Conference* (July 2012), pp. 750–759. doi:10.1109/SRII.2012.110. 2

[dABM*18] DE ALVARENGA S. C., BARBON S., MIANI R. S., CUKIER M., ZARPELÃO B. B.: Process mining and hierarchical clustering to help intrusion alert visualization. *Computers & Security 73* (Mar. 2018), 474–491. doi:10.1016/j.cose.2017.11.021. 2

[dLM17] DE LEONI M., MARRELLA A.: Aligning Real Process Executions and Prescriptive Process Models through Automated Planning. *Expert Syst. Appl. 82* (2017), 162–183. doi:10.1016/j.eswa.2017.03.047. 1, 2

[DZSC18] DUAN L., ZHANG Y., SUN C.-A., CHEN J.: Enforcing compliance of hierarchical business process with visual security constraints. *Int. Journal of System Assurance Engineering and Management 9* (2018), 703–715. doi:10.1007/s13198-017-0653-1. 2

[EF08] ECKLEDER A., FREYTAG T.: Woped a tool for teaching, analyzing and visualizing workflow nets. *Petri Net Newsletter* (2008). 2

[Eni23] ENISA: Good Practice Guide for Incident Management, 2023. 1, 2

[FHBM12] FELDERER M., HAISJACKL C., BREU R., MOTZ J.: Integrating manual and automatic risk assessment for risk-based testing. In *International Conference on Software Quality* (2012), pp. 159–180. doi:10.1007/978-3-642-27213-4_11. 1

[FPB*17] FRANKLIN L., PIRRUNG M., BLAHA L., DOWLING M., FENG M.: Toward a visualization-supported workflow for cyber alert management using threat models and human-centered design. In *2017 IEEE Symposium on Visualization for Cyber Security (VizSec)* (2017), pp. 1–8. doi:10.1109/VIZSEC.2017.8062200. 2

[Fur86] FURNAS G. W.: Generalized fisheye views. *Acm Sigchi Bulletin 17*, 4 (1986), 16–23. 3

[Gov21] GOVE R.: Automatic Narrative Summarization for Visualizing Cyber Security Logs and Incident Reports. In *2021 IEEE Symposium on Visualization for Cyber Security (VizSec)* (Oct. 2021), pp. 1–9. ISSN: 2639-4332. doi:10.1109/VizSec53666.2021.00005. 2

[HN98] HINTZE J. L., NELSON R. D.: Violin plots: a box plot-density trace synergism. *The American Statistician 52*, 2 (1998), 181–184. 4

[ID91] INSELBERG A., DIMSDALE B.: Parallel coordinates. In *Human-Machine Interactive Systems*. Springer, 1991, pp. 199–233. 4

[Ins07] INSTITUTE I. G.: *Cobit 4.1*. ISA, 2007. 2

[ISO13] *Part 1: Principles of incident management; Part 2: Guidelines to plan and prepare for incident response; Part 3: Guidelines for ICT incident response operations*. Standard, International Organization for Standardization, Geneva, CH, Mar. 2013. 1, 2, 4

[IT 19] IT GOVERNANCE INSTITUTE (Ed.): *CobiT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models*. IT Governance Institute, Rolling Meadows, 2019. 1

[KKG20] KODITUWAKKU H. A. D. E., KELLER A., GREGOR J.: InSight2: A Modular Visual Analysis Platform for Network Situational Awareness in Large-Scale Networks. *Electronics 9*, 10 (Oct. 2020), 1747. Number: 10 Publisher: Multidisciplinary Digital Publishing Institute. doi:10.3390/electronics9101747. 2

[KRK17] KNUPLESCH D., REICHERT M., KUMAR A.: A framework for visually monitoring business process compliance. *Information Systems 64* (2017), 381–409. doi:10.1016/j.is.2016.10.006. 2

[MCB*17] MCCORMAC A., CALIC D., BUTAVICIUS M., PARSONS K., ZWAANS T., PATTINSON M., ET AL.: A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems 21* (2017). doi:10.3127/ajis.v21i0.1697. 1

[Mik21] MIKSCH S.: Visual analytics meets process mining: Challenges and opportunities. In *2021 3rd International Conference on Process Mining (ICPM)* (2021), pp. xiv–xiv. doi:10.1109/ICPM53251.2021.9576854. 2

[NBS17] NOVIKOVA E. S., BEKENEVA Y. A., SHOROV A. V.: Towards visual analytics tasks for the security information and event management. In *2017 Int. Conf. "Quality Management,Transport and Information Security, Information Technologies" (IT QM IS)* (Sept. 2017), pp. 90–93. doi:10.1109/ITMQIS.2017.8085770. 2

[NG09] NATARAJAN S., GANZ A.: Distributed visual analytics for collaborative emergency response management. In *2009 Annual International Conference of the IEEE Engineering in Medicine and Biology Society* (Sept. 2009), pp. 1714–1717. ISSN: 1558-4615. doi:10.1109/IEMBS.2009.5333481. 2

[NIS21] NIST: Nist special publication 800-61, revision 2, computer security incident handling guide, 2021-04-23 2021. 2

[Pet66] PETRI C. A.: *Communication with automata*. Tech. rep., Hamburg University, 1966. 2

[RER*10] RASMUSSEN J., EHRLICH K., ROSS S., KIRK S., GRUEN D., PATTERSON J.: Nimble cybersecurity incident management through visualization and defensible recommendations. VizSec '10, ACM, pp. 102–113. doi:10.1145/1850795.1850807. 2

[RPC*00] RUTHERFORD K., PARKHILL J., CROOK J., HORSNELL T., RICE P., RAJANDREAM M.-A., BARRELL B.: Artemis: sequence visualization and annotation. *Bioinformatics 16* (2000), 944–945. 3, 4

[SA82] SPENCE R., APPERLEY M.: Data base navigation: an office environment for the professional. *Behaviour & Information Technology 1*, 1 (1982), 43–54. doi:10.1080/01449298208914435. 3

[Ser16] *ServiceNow-TM*. Standard, Gildesoft, USA, June 2016. 2, 4

[vdA16] VAN DER AALST W. M. P.: *Data Science in Action*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016. 1

[vdAdLtH11] VAN DER AALST W. M., DE LEONI M., TER HOFSTEDE A. H.: Process mining and visual analytics: Breathing life into business process models. *BPM Center Report BPM-11-15, BPMcenter. org 17* (2011), 699–730. 2