Cyber Security for Business Processes: Automating Security Enhancement Along Process Lifecycle

Moshe Hadad[1]

[1]Department of Information Systems, University of Haifa, Israel, Abba Khoushy Ave 199, Haifa, 3498838

Abstract

This research focuses on improving security for business processes by developing automated methods for threat modeling, security requirements and countermeasure generation, and operational reassessment of security needs along the lifecycle of a business process. We propose an automated approach that uses large language models (LLMs), security frameworks, and cyber threat intelligence (CTI) to dynamically assess and secure business processes as they evolve. The preliminary results indicate an improved efficiency in identifying and mitigating cyber threats compared to traditional methods.

Keywords

Business Processes, Threat Modeling, Security Requirements, Process Monitoring

1. Introduction

The frequency of cyber attacks targeting organizations has almost doubled in recent years[1, 2, 3], primarily due to the accelerated pace of digital transformation during the COVID-19 pandemic and the emergence of generative AI and large language models (LLMs). These advancements have expanded both the attack surface and the arsenal of tools available to adversaries[4]. Such developments highlight the critical importance of addressing security as early as possible[2, 1], by embedding it directly into the design of a business process (BP). Early integration ensures that security and business requirements are considered from the start[5, 6].

However, existing approaches often fail to address the dynamic nature of business environments. They emphasize security requirements at the design phase, rely on manual and time-intensive processes, and fail to adapt as BPs and threat landscape change. Consequently, security assesment becomes obsolete. As highlighted by [7], there is a need for methodologies that ensure security is maintained across the entire BP lifecycle.

This research will propose an approach for maintaining security throughout the lifecycle of BPs by automating threat modeling, security requirement collection, and countermeasure suggestion at the design phase, with continuous monitoring during BP operation as it evolves. We use LLMs with BPMN process models, to enhance automation, while mitigating LLM limitations through cybersecurity knowledge bases such as MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK)[1] and DEF3ND[2]. Additionally, we leverage CTI data and BP event logs for ongoing security assessment.

Four challenges emerge when automating security across BP lifecycles: (1) Bridging abstraction layers between security frameworks (ATT&CK/D3FEND) and process models requires novel mapping techniques to align tactical MITRE techniques with BPMN elements. (2) These frameworks are comprehensive. Efficient methods are required for processing and identifying BPM relevant aspects (3) LLM automation faces inherent limitations: e.g. hallucinations, inconsistencies, and lack of domain

23rd International Conference on Business Process Management (BPM 2025), August 31–September 5, 2025, Seville, Spain

mhadad24@campus.haifa.ac.il (M. Hadad)

0000-0002-9315-6260 (M. Hadad)

[1]ATTA&CK is a knowledge base of adversary tactics and techniques based on real-world observations developed by the MITRE Corporation https://attack.mitre.org/

[2]D3FEND is a knowledge graph of cybersecurity countermeasures developed by the MITRE Corporation https://d3fend.mitre.org/

knowledge. (4) Continuous security alignment demands real-time correlation of CTI feeds with process execution logs.

The research goals are to develop methods for : 1) Automating threat modeling, security requirement collection, and countermeasure suggestion for BP security at the design phase. 2) Monitoring and reassessing BP security needs facing process and environment changes. This research extends current knowledge by leveraging cutting-edge technologies to automate security activities across the entire BP lifecycle.

2. Related Work

In this section, we explore the literature in the areas of threat modeling, security requirements, and BP monitoring. In addition, we review recent work of applying LLM for BP and for security.

For threat modeling, Von der Assen et al.[8] proposed an approach focused on detecting insider threats by mapping BPMN elements to threat events. Granata et al.[9] enhanced threat modeling for e-Government processes using the European Union Agency for Cybersecurity (ENISA)[3] threat landscape, while Hacks et al.[10] introduced BPMN2MAL, enabling attack simulations by translating BPMN elements. Although these methods have made progress in automating threat modeling, they remain limited by their dependence on manual configuration, lack of scalability, and the absence of integration with threat intelligence during the operational phase.

In the domain of security requirements and countermeasures, several approaches have aimed to extend modeling languages for security. Notably, [7] emphasized formalizing security requirements, while Zareen et al.[11] and Lins et al. [12] proposed frameworks integrating security into BP models. However, these methods primarily focus on the design phase and lack automation, requiring manual intervention. Approaches by Rodriguez et al.[13], Menzel et al.[14], Turki et al.[15] similarly target design-phase security but do not extend to ongoing process adaptation. Additional studies, such as Saleem et al.[16], Mülle et al.[17], and Ahmed et al.[18, 19], further addressed security integration, yet these also predominantly focus on static design-phase measures and lack full automation.

BP monitoring for security has also been studied, with Ramadan et al.[20, 21], Varela-Vaca et al.[22] and Asim et al.[23] proposing methods for detecting conflicts and verifying security policies in BPMN-based processes. Salnitri et al.[24, 25] introduced SecBPMN2, a framework for specifying and verifying security policies. Yet, these approaches are primarily static, focusing on design-phase security enhancement rather than continuous monitoring at an operational-phase.

Finally, Large Language Models (LLMs) have emerged as a tool for automating security tasks. Elsharef et al.[26] applied LLMs for threat identification, while Wornow et al.[27] explored LLMs for general BP analysis. Despite these advances, existing works do not fully integrate LLMs for continuous security analysis across the BP lifecycle.

In conclusion, while existing approaches have made significant strides in automating various aspects of BP security, there remains a need for methods that can provide flexible, automated, and scalable solutions for security activities in complex business environments, particularly those that can integrate operational-phase CTI data and adapt to evolving processes.

3. Research questions

Our primary research question is: **"How can a proactive, process-centric security approach enhance BP security throughout its lifecycle, from design to execution and monitoring?"** This question can be broken down into the following research questions:

1. **RQ1 : How can threat modeling be automated and applied iteratively to enhance BP security along process lilfecycle?**

[3] https://www.enisa.europa.eu/

- This question aims to develop a method for automated BP threat modeling which is aware of and tailored to the specific business processes. It involves creating strategies and controls to identified threats across design and operational phases.

2. **RQ2 :How can security requirements and countermeasures be systematically analyzed, designed, and integrated into business processes during the early design phase?**
    - This question explores the generation of security requirements and countermeasures for BPs. It involves developing a systematic method to analyze, design, and integrate security requirements and countermeasures for a business process given its BPMN and process specification.
3. **RQ3 : How can we reassess the security needs of a business process based on Cyber Threat Intelligence (CTI) and process execution data to support continuous monitoring at the operational phase**
    - This question focuses on reassessing the security needs of a business processes. It involves identifying the specific types of CTI and processes data that should be used to facilitate the monitoring.

By addressing these research questions, This study aims to enhance BP security by using LLMs, security frameworks, and CTI data to support security analysis, design, and integration. It also enables dynamic monitoring to identify and apply countermeasures throughout the BP lifecycle.

4. Methodology

This research adopts the design science research methodology articulated by [28].

For the identification and motivation of the problem, we performed a comprehensive literature review on BP security. This revealed three core limitations: 1) manual-intensive threat modeling processes that scale poorly for complex BPs , 2) static security requirements that fail to adapt to evolving operational contexts, and 3) insufficient integration of real-time cyber threat intelligence (CTI) with process execution data for monitoring.

Through an iterative analysis of these gaps, we designed a conceptual framework for BP security, as a main objective (Fig.1). This framework is composed of the following envisioned artifacts:

1. A1) A method for continuous automatic threat modeling across BP lifecycle phases.
2. A2) A method for automatic BP security requirements and countermeasure suggestions.
3. A3) A method to link between CTI data and BP model event logs
4. A4) A method for dynamically monitoring for BP security under evolving process and threat conditions.

In our design and development process, we will use both top-down and bottom-up approaches for all artifacts. For A1 and A2, the top-down approach analyzes existing techniques and develops LLM-based methods, while the bottom-up approach applies these methods to BPMN examples, compares the results with domain experts, and iteratively refines them. For A3, the top-down approach reviews event log formats, CTI data standards, and ontologies to design a metamodel linking CTI data to event logs. The bottom-up approach uses simulated environments to generate data, conducts experiments with various security events, and iteratively improves the method. For A4, the top-down approach examines security monitoring methods and frameworks like ATT&CK and D3FEND, developing algorithms to reassess threat models using linked data. The bottom-up approach implements BPs with predefined security measures in simulations, induces security violations, analyzes the resulting event logs, refines algorithms, and develops visualization techniques for findings.

For evaluation, each artifact will be evaluated through a case study involving domain experts. The evaluation process involves selecting suitable BPs, establishing ground truths with domain experts, applying the proposed methods, and comparing the results against updated ground truths. In addition, the data will be used to conduct experiments that compare different approaches to solve the problem.

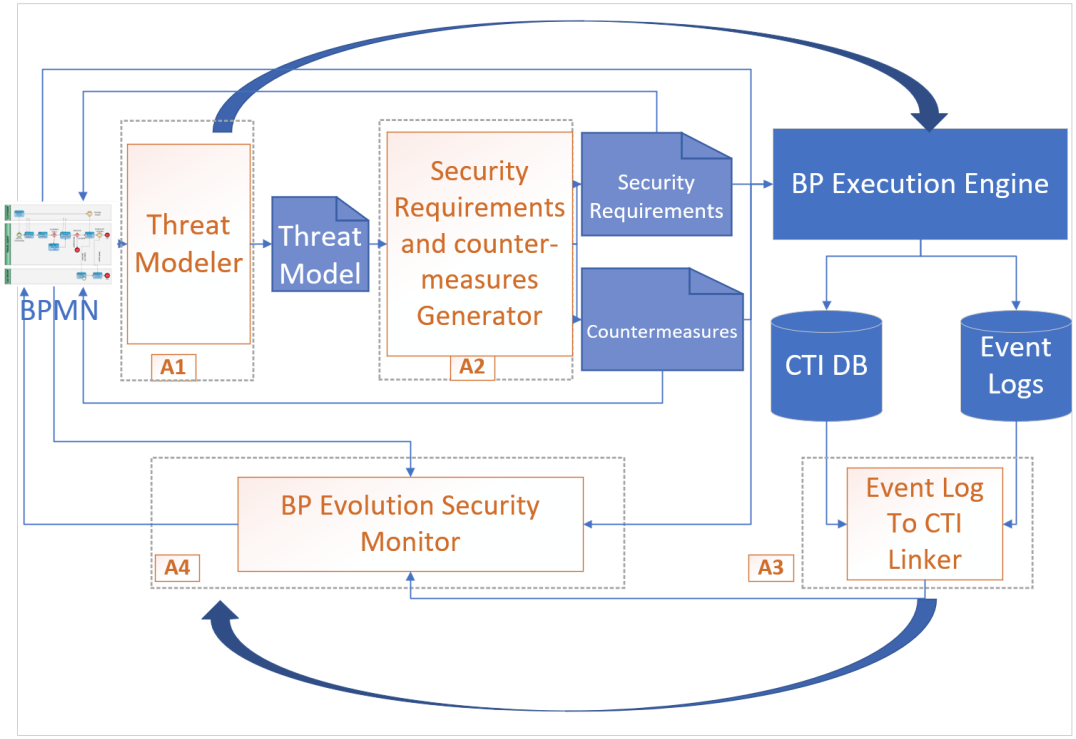

Figure 1: BP Security Framework

5. Preliminary Results

We conducted two experiments with threat modeling approaches to explore the challenges of automating it using LLM and bridging abstraction layers between security frameworks (ATT&CK/D3FEND) and process models.

Experiment A: Design-phase threat modeling, comparing an ad-hoc LLM-based method and a state-of-the-art knowledge based approach (KBA) [8]. Both methods start by identifying the assets that participate in the process and then identify associated threats. As an ad-hoc LLM-based method, we applied prompt engineering to a BPMN sourced from [8] and compared the indicated assets and threats with those identified by the KBA. The asset identification step yielded 13 assets in both cases, with slight variations in recognition. Our LLM-based method identified 40 threats compared to 36 identified by KBA. Notably, the LLM-based approach uncovered additional threats, such as injection attacks, unauthorized lookups, and sending to unauthorized recipients or tampering (a form of privilege escalation). These threats were absent in the KBA's results, as acknowledged by [8] in their evaluation with domain experts. In summary, our prompt engineering approach outperformed KBA in comprehensive threat identification and in its full automation.

Experiment B: Operational-phase threat modeling, focused on correlating CTI data with its corresponding event log and connecting them to the D3FEND's Digital Artifact Ontology (DAO), followed by refinement using LLM. DAO serves as a link between the ATT&CK framework, which models threats, and the D3FEND knowledge graph, which models countermeasures. The main idea is to link a BP event log to the DAO to map activities to threats and countermeasures, enriching threat model and security requirements done at design time. To this end, we used the HR recruitment BP event log from [29] [4],

[4]https://github.com/HaifaUniversityBPM/traffic-data-to-event-log

which contains HTTP data. HTTP request and response represent a small portion of CTI data because they capture specific network-level interactions that can reveal indicators of compromise. We systematically gathered all HTTP communication data associated with each activity in the event log. These network-level data served as input for the D3FEND artifact extractor [5], which automatically identified digital artifacts from the DAO for the given HTTP data. This established a connection between BP activities and multiple potential threats via the DAO's relationship with the ATT&CK matrix. Through this chain relationship, we automatically associated each activity with its relevant ATT&CK-identified threats producing a threat model. To refine the threat modeling process, we implemented prompt engineering techniques, providing the LLM with the identified potential threats and the BPMN diagram, while instructing it to apply the STRIDE[6] methodology. This approach resulted in a refined and detailed threat model, which offers specific threat mappings for each activity within the BPMN. In summary, this experiment shows how CTI data can be connected to event logs and facilitate the threat modeling process that involves security knowledge bases in combination with LLM.

In conclusion, this research contributes to the existing body of knowledge by proposing to automate security activities throughout the BP lifecycle, by leveraging LLMs, security frameworks, and CTI data. The preliminary results show promising potential. Future work will focus on refining the proposed methods, addressing limitations in LLMs outputs, and enhancing the precision of threat and countermeasure mappings. These efforts are expected to advance the field of automated BP security and provide valuable insights for academic and practical applications.

Declaration on Generative AI

During the preparation of this work, the author used Perplexity with GPT-4 to: Paraphrase and reword, Grammar and spelling check, Improve writing style and Abstract drafting. The author then reviewed, edited, and assumes full responsibility for the publication's content.

References

[1] R. Rupeika-Apoga, K. Petrovska, L. Bule, The effect of digital orientation and digital capability on digital transformation of smes during the covid-19 pandemic, Journal of Theoretical and Applied Electronic Commerce Research 17 (2022) 669–685.

[2] D. Savić, Covid-19 and work from home: Digital transformation of the workforce, Grey Journal (TGJ) 16 (2020) 101–104.

[3] J. J. Paolo Dal Cin, Global cybersecurity outlook 2023, https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf, 2023. Accessed: 2023-01-01.

[4] M. Gupta, C. Akiri, K. Aryal, E. Parker, L. Praharaj, From chatgpt to threatgpt: Impact of generative ai in cybersecurity and privacy, IEEE Access 11 (2023) 80218–80245. doi:10.1109/ACCESS.2023.3300381.

[5] E. Goettelmann, N. Mayer, C. Godart, Integrating security risk management into business process management for the cloud, in: 2014 IEEE 16th Conference on Business Informatics, volume 1, IEEE, 2014, pp. 86–93.

[6] A. D. Brucker, I. Hang, G. Lückemeyer, R. Ruparel, Securebpmn: Modeling and enforcing access control requirements in business processes, in: Proceedings of the 17th ACM symposium on Access Control Models and Technologies, 2012, pp. 123–126.

[7] N. Soveizi, F. Turkmen, D. Karastoyanova, Security and privacy concerns in cloud-based scientific and business workflows: A systematic review, Future Generation Computer Systems 148 (2023) 184–200.

[8] J. von der Assen, J. Hochuli, T. Grübl, B. Stiller, The danger within: Insider threat modeling using business process models, arXiv preprint arXiv:2406.01135 (2024).

[5] https://d3fend.mitre.org/tools/artifact-extracto

[6] https://en.wikipedia.org/wiki/STRIDE_model

[9] D. Granata, M. Rak, G. Salzillo, G. Di Guida, S. Petrillo, Automated threat modelling and risk analysis in e-government using bpmn, Connection Science 35 (2023) 2284645.
[10] S. Hacks, R. Lagerström, D. Ritter, Towards automated attack simulations of bpmn-based processes, in: 2021 IEEE 25th International Enterprise Distributed Object Computing Conference (EDOC), IEEE, 2021, pp. 182–191.
[11] S. Zareen, A. Akram, S. Ahmad Khan, Security requirements engineering framework with bpmn 2.0. 2 extension model for development of information systems, Applied Sciences 10 (2020) 4981.
[12] F. A. Lins, E. T. Sousa, N. S. Rosa, A survey on automation of security requirements in service-based business processes, International Journal of Web Engineering and Technology 13 (2018) 3–29.
[13] A. Rodríguez, E. Fernández-Medina, J. Trujillo, M. Piattini, Secure business process model specification through a uml 2.0 activity diagram profile, Decision Support Systems 51 (2011) 446–465.
[14] M. Menzel, R. Warschofsky, I. Thomas, C. Willems, C. Meinel, The service security lab: A model-driven platform to compose and explore service security in the cloud, in: 2010 6th World Congress on Services, IEEE, 2010, pp. 115–122.
[15] S. H. Turki, F. Bellaaj, A. Charfi, R. Bouaziz, Modeling security requirements in service based business processes, in: International Workshop on Business Process Modeling, Development and Support, Springer, 2012, pp. 76–90.
[16] M. Saleem, J. Jaafar, M. Hassan, A domain-specific language for modelling security objectives in a business process models of soa applications, AISS 4 (2012) 353–362.
[17] J. Mülle, S. Von Stackelberg, K. Böhm, A security language for BPMN process models, KIT, Fakultät für Informatik, 2011.
[18] N. Ahmed, R. Matulevicius, A method for eliciting security requirements from the business process models., in: CAiSE (Forum/Doctoral Consortium), volume 1164, 2014, pp. 57–64.
[19] N. Ahmed, R. Matulevičius, Securing business processes using security risk-oriented patterns, Computer Standards & Interfaces 36 (2014) 723–733.
[20] Q. Ramadan, D. Strüber, M. Salnitri, J. Jürjens, V. Riediger, S. Staab, A semi-automated bpmn-based framework for detecting conflicts between security, data-minimization, and fairness requirements, Software and Systems Modeling 19 (2020) 1191–1227.
[21] Q. Ramadan, D. Strüber, M. Salnitri, V. Riediger, J. Jürjens, Detecting conflicts between data-minimization and security requirements in business process models, in: Modelling Foundations and Applications: 14th European Conference, ECMFA 2018, Held as Part of STAF 2018, Toulouse, France, June 26-28, 2018, Proceedings 14, Springer, 2018, pp. 179–198.
[22] Á. J. Varela-Vaca, L. Parody, R. M. Gasca, M. T. Gómez-López, Automatic verification and diagnosis of security risk assessments in business process models, IEEE Access 7 (2019) 26448–26465.
[23] M. Asim, A. Yautsiukhin, A. D. Brucker, T. Baker, Q. Shi, B. Lempereur, Security policy monitoring of bpmn-based service compositions, Journal of Software: Evolution and Process 30 (2018) e1944.
[24] M. Salnitri, F. Dalpiaz, P. Giorgini, Designing secure business processes with secbpmn, Software & Systems Modeling 16 (2017) 737–757.
[25] M. Salnitri, F. Dalpiaz, P. Giorgini, Modeling and verifying security policies in business processes, in: International Workshop on Business Process Modeling, Development and Support, Springer, 2014, pp. 200–214.
[26] I. Elsharef, Z. Zeng, Z. Gu, Facilitating threat modeling by leveraging large language models, in: Workshop on AI Systems with Confidential Computing, 2024.
[27] M. Wornow, A. Narayan, B. Viggiano, I. S. Khare, T. Verma, T. Thompson, M. A. F. Hernandez, S. Sundar, C. Trujillo, K. Chawla, et al., Wonderbread: A benchmark for evaluating multimodal foundation models on business process management tasks, arXiv preprint arXiv:2406.13264 (2024).
[28] A. R. Hevner, S. T. March, J. Park, S. Ram, Design science in information systems research, MIS quarterly (2004) 75–105.
[29] M. Hadad, G. Engelberg, P. Soffer, From network traffic data to a business-level event log, in: International Conference on Business Process Modeling, Development and Support, Springer, 2023, pp. 60–75.