Simulation of Cyber Incident Response Using Artificial Intelligence

Dmitrij Kolodynskij, Nikolaj Goranin
Department of Information Systems, Faculty of Fundamental Sciences, VILNIUS TECH

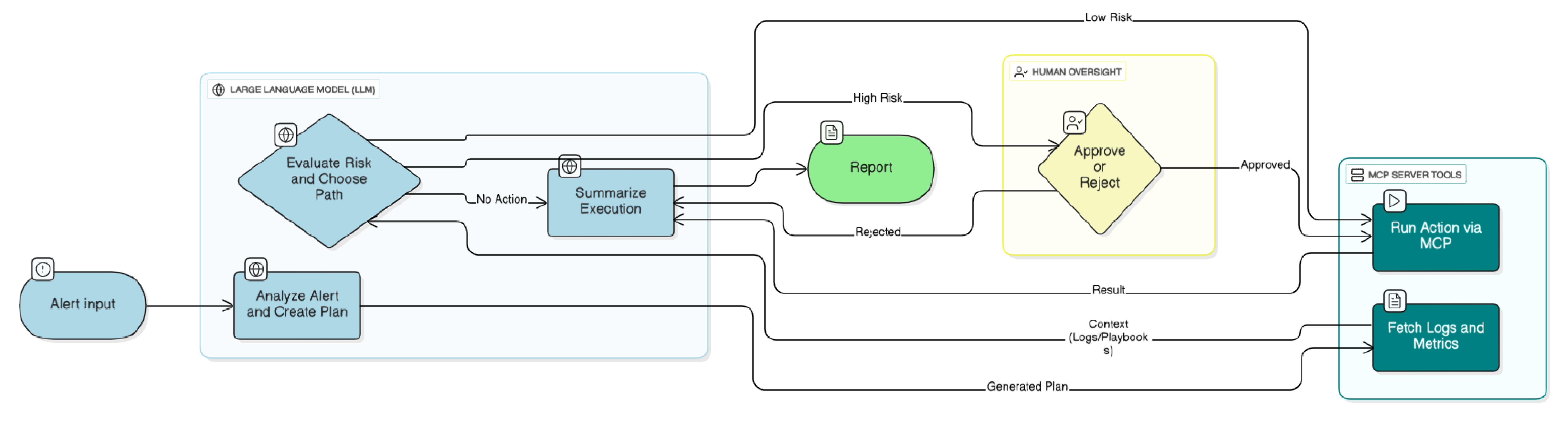
INTRODUCTION

- Modern cybersecurity operations face increasing complexity, where static playbooks are often insufficient to handle dynamic and evolving threats. This research explores the simulation of cyber incident response using Generative Artificial Intelligence to create adaptive, data-driven response frameworks. The proposed approach employs LLMs to automatically generate incident scenarios and response plans, simulating real-world decision-making under controlled conditions. By integrating AI-driven reasoning with mock operational environments, the simulation enables experimentation with various response strategies - ranging from automated execution to human-in-the-loop decision paths.
- From an organizational perspective, cyberattacks are inevitable for a variety of reasons — organizations cannot identify every possible vulnerability in their systems and cannot fully eliminate the human factor, often regarded as the weakest link in cybersecurity. Incident response capabilities enable affected companies to detect, contain, and recover from security incidents efficiently, while well-structured response scenarios also support the wider community by helping to prevent similar attacks in the future. In this context, the generation of incident response plans through AI-based simulation becomes a practical necessity: it allows organizations to proactively develop, test, and refine their response strategies in a controlled, risk-free environment. This capability is essential for reducing response times, enhancing coordination among security operations teams, and improving overall cyber resilience.
- Developing sandboxed simulation environments allows organizations to test response frameworks safely. Simulations enable high-fidelity testing of strategies without affecting live systems, while allowing AI models to improve through iterative learning and data aggregation.
- Current challenge:
  - Traditional cybersecurity relies on static playbooks that fail to adapt to dynamic, evolving threats.
  - Organizations struggle to test response strategies safely and scale operations due to limitations of manual execution.
  - Incident response analysts are burdened with repetitive tasks (e.g., identifying false positives, coordinating responses), which can lead to cognitive fatigue, reducing both the speed and accuracy of decision-making processes.

OVERVIEW

- The integration of Generative AI into incident management is an active area of research, with significant methodological advances occurring in both physical and digital domains. In the context of traffic management, Almohammad and Georgakis [4] explored the use of pre-defined generative templates to create automated response plans, highlighting the necessity of tailoring scenarios to specific situational variables—a principle that parallels the need for bespoke mitigation strategies in cybersecurity. Expanding on this, the IncidentResponseGPT [5] framework introduces a novel system where Generative AI synthesizes region-specific guidelines to expedite decision-making, utilizing the TOPSIS method to rank generated plans based on resource efficiency and impact minimization.
- Transposing these adaptive capabilities to the cyber domain, Loumachi et al. [6] addressed the challenge of forensic accuracy through Retrieval-Augmented Generation (RAG). Their work demonstrates that integrating real-time data retrieval with Large Language Models allows for the precise reconstruction of incident timelines, ensuring that generative outputs are grounded in actual forensic evidence. On a strategic level, recent studies on LLM-driven Incident Response Planning (IRP) argue that models like ChatGPT [7] can overcome resource constraints caused by high turnover and legacy technology; by identifying documentation gaps and suggesting best practices, LLMs significantly streamline the drafting and refinement of comprehensive IRPs.
- Moving from planning to execution, Akbari et al. [8] investigate the transition of static, semi-structured playbooks into fully automated, AI-supported structures, a shift that enhances regulatory compliance and facilitates the sharing of best practices across organizations. Finally, operational frameworks such as AI4SOAR illustrate the practical convergence of these technologies with Security Orchestration, Automation, and Response (SOAR) tools [9]. By employing AI-based similarity learning to map security events into automated workflows, AI4SOAR reduces dependency on human operators for routine tasks and ensures a consistent, standardized response to security incidents.

PROPOSED WORKFLOW OF THE AI-BASED INCIDENT RESPONSE PLAN SIMULATOR



EXAMPLES OF SIMULATION SCENARIOS

Scenario	Incident	AI Action	Decision	Outcome	Result
Autonomous Resilience (ALERT-1001)	Database CPU Saturation (>95%).	Matches symptoms to "CPU Saturation" playbook.	Low Risk (Rule-based).	Automatically executes . scale_instance	Incident resolved in seconds without human intervention.
Human-Centric Safety (ALERT-1002)	Post-deployment HTTP 500 Error Spike.	Identifies correlation with recent deployment. Proposes . rollback_deployment	High Risk (Policy Enforcement).	Routes to HITL node. Waits for approval before executing.	Safe recovery preventing accidental service disruption.

RESULTS AND CONCLUSIONS

- This project demonstrates the potential of using large language models, specifically Google Gemini, to augment and simulate cyber incident response workflows, providing a cognitive layer to traditional automation.
- By integrating AI-driven reasoning with structured decision-making, the system dynamically generates response plans, retrieves context from logs and metrics, and evaluates risk against predefined policies.
- The approach enables adaptive execution strategies, seamlessly switching between fully automated remediation, human-in-the-loop (HITL) escalation, or informational summarization based on risk assessment.
- The simulation environment provides a safe sandbox for organizations to test, refine, and validate their response strategies without exposing live infrastructure to risk.
- Although currently only a concept, this work illustrates a scalable framework for intelligent cyber defense, suggesting that combining artificial intelligence with controlled management can significantly expand the capabilities of security operations centers (SOCs).

DAMSS
DATA ANALYSIS METHODS FOR SOFTWARE SYSTEMS

16th Conference
Druskininkai, Lithuania, Hotel „Europa Royale"
November 27 – 29, 2025
http://www.mii.vu.lt/DAMSS

VILNIUS TECH
Fundamentinių mokslų fakultetas

REFERENCES

1. Tashfeen MTA. Building blocks of incident response: Security operation centers. AIP Conf Proc [Internet]. American Institute of Physics Inc.; 2023 [cited 2025 Nov 24];2814. https://doi.org/10.1063/5.0148860/2901924

2. Nyre-Yu M, Gutzwiller RS, Caldwell BS. OBSERVING CYBER SECURITY INCIDENT RESPONSE:QUALITATIVE THEMES FROM FIELD RESEARCH. Proceedings of the Human Factors and Ergonomics Society [Internet]. SAGE Publications Inc.; 2019 [cited 2025 Nov 24];63:437–431. https://doi.org/10.1177/1071181319631016;ISSUE:ISSUE:DOI

3. Ricks M. Building capability and community through cyber-incident response exercises. J Bus Contin Emer Plan. Henry Stewart Publications; 2024;18:49–58. https://doi.org/10.69554/GCZJ1400

4. Rojas I, Pomares H, Herrera LJ, Rojas F, Valenzuela O, Almohammad A, et al. Automated Approach for Generating and Evaluating Traffic Incident Response Plans. Engineering Proceedings 2023, Vol 39, Page 13 [Internet]. Multidisciplinary Digital Publishing Institute; 2023 [cited 2025 Nov 24];39:13. https://doi.org/10.3390/ENGPROC2023039013

5. Grigorev A, Saleh A-SMK, Ou Y. IncidentResponseGPT: Generating Traffic Incident Response Plans with Generative Artificial Intelligence. 2024 [cited 2025 Nov 24]; https://arxiv.org/pdf/2404.18550. Accessed 24 Nov 2025

6. Loumachi FY, Ghanem MC, Ferrag MA. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models. Computers 2025, Vol 14, Page 67 [Internet]. Multidisciplinary Digital Publishing Institute; 2025 [cited 2025 Nov 24];14:67. https://doi.org/10.3390/COMPUTERS14020067

7. Hays S, White J. Employing LLMs for Incident Response Planning and Review. 2024 [cited 2025 Nov 24]; https://arxiv.org/pdf/2403.01271. Accessed 24 Nov 2025

8. Akbari Gurabi M, Nitz L, Bregar A, Popanda J, Siemers C, Matzutt R, et al. Requirements for Playbook-Assisted Cyber Incident Response, Reporting and Automation. Digital Threats: Research and Practice [Internet]. Association for Computing Machinery; 2024 [cited 2025 Nov 24];5:34. https://doi.org/10.1145/3688810;CSUBTYPE:STRING:JOURNAL;SUBPAGE:STRING:FULL

9. Nguyen MD, Mallouli W, Cavalli AR, Montes De Oca E. AI4SOAR: A Security Intelligence Tool for Automated Incident Response. ACM International Conference Proceeding Series [Internet]. Association for Computing Machinery; 2024 [cited 2025 Nov 24]; https://doi.org/10.1145/3664476.3670450;PAGE:STRING:ARTICLE/CHAPTER