

ENG 211 C 34859

Abdias Noel

August 17, 2026

Research Proposal

Introduction

Enterprises of all sizes face cybersecurity threats that can compromise sensitive information, interrupt business operations, create financial losses, and damage an organization's reputation and customer trust. Phishing attacks, ransomware, unauthorized access, and unsanctioned disclosure are among the threats organizations must continuously prepare for and respond to. Because cyberattacks can occur at any time, an organization's ability to quickly identify and respond to suspicious activity can be an important part of limiting the damage caused by a successful attack.

One approach organizations use to address these threats is continuous security monitoring. Continuous monitoring uses technologies such as Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR) to collect and analyze security information and identify potentially malicious activity as it occurs. Rather than relying exclusively on security assessments conducted at specific intervals, continuous monitoring is intended to provide organizations with current visibility into their systems and security events.

However, implementing and maintaining these technologies can require significant financial, technological, and human resources. Their adoption therefore raises an important question for enterprises: Do continuous monitoring practices produce measurable improvements in cybersecurity outcomes? Examining outcomes such as successful compromise rates, detection time, containment time, and remediation time can help determine whether continuous monitoring actually improves an organization's ability to detect and respond to cyber incidents.

Problem statement

Companies invest significant resources in cybersecurity professionals, security technologies, and monitoring systems to prevent and respond to cyber threats. However, organizations may differ considerably in how quickly they detect incidents, how successfully they contain them, and how effectively they recover from them. Delayed detection can provide attackers with additional time to compromise systems, access sensitive information, or disrupt business operations.

Although continuous monitoring is intended to provide greater awareness of security events and allow organizations to respond more quickly, the presence of monitoring technology alone does

not necessarily demonstrate that an organization's security has improved. It is therefore important to examine measurable security outcomes to determine whether enterprises using continuous monitoring experience fewer successful attacks and faster incident response than organizations that do not use comparable monitoring practices.

Research question

To what extent does continuous monitoring reduce successful cyber-attacks and incident response time in an enterprise environment?

Purpose

The purpose of the study is to determine whether enterprises with continuous monitoring practices experience fewer successful attacks and respond to cybersecurity incidents faster than enterprises without comparable continuous monitoring practices. The study will examine measurable indicators of cybersecurity performance, including attack detection, successful compromise rates, incident detection time, containment rates, and remediation time.

Methodology

This study will use a qualitative and comparative review of existing cybersecurity research and publicly available evidence. Sources will include peer-reviewed cybersecurity research, case studies, public incident reports, industry reports, and relevant cybersecurity standards and compliance guidelines.

Sources will be evaluated based on their credibility, relevance to enterprise cybersecurity, and their ability to provide measurable information related to continuous monitoring and incident response. Where available, the study will compare organizations or incidents involving continuous monitoring practices with those involving limited or less-developed monitoring capabilities.

The collected information will be examined for relationships between continuous monitoring and several cybersecurity outcomes, including attack detection, successful compromise rates, incident detection time, containment rates, and remediation time. These comparisons will be used to determine whether the available evidence indicates that continuous monitoring contributes to fewer successful attacks and faster incident response and recovery.

References

- Ali, G., et al. (2025). Enhancing cybersecurity incident response: AI-driven approaches, challenges, and future directions. *Results in Engineering*, 25, Article 104078. <https://doi.org/10.1016/j.rineng.2025.104078>
- Cybersecurity and Infrastructure Security Agency. (n.d.). *Continuous diagnostics and mitigation (CDM) program*. Retrieved July 29, 2026, from <https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>
- Dempsey, K. L., Witte, G. A., Rike, D. M., & Witte, R. S. (2011). *Information security continuous monitoring (ISCM) for federal information systems and organizations* (NIST Special Publication 800-137). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-137>
- European Union Agency for Cybersecurity. (2020). *How to set up CSIRT and SOC*. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20How%20to%20set%20up%20CSIRT%20and%20SOC.pdf>
- Forsberg et al. (2023), Technical performance metrics of a security operation center. *Computers & Security*, 135, Article 103529. <https://doi.org/10.1016/j.cose.2023.103529>
- González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), Article 4759. <https://doi.org/10.3390/s21144759>
- IBM. (2025). *Cost of a data breach report 2025*. <https://www.ibm.com/reports/data-breach>
- Tariq, S., Chhetri, M. B., Nepal, S., & Paris, C. (2025). Alert fatigue in security operations centres: Research challenges and opportunities. *ACM Computing Surveys*, 57(9), Article 224. <https://doi.org/10.1145/3723158>
- Verizon. (2025). *2025 data breach investigations report*. <https://www.verizon.com/business/resources/reports/2025-dbir-data-breach-investigations-report.pdf>

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8, 227756–227779.
<https://doi.org/10.1109/ACCESS.2020.3045514>