

The Effectiveness of Continuous Monitoring in Enterprise Cybersecurity

Abdias Noel

Old Dominion University

ENGL 211

Mr. Norris

August 17, 2026

The Effectiveness of Continuous Monitoring in Enterprise Cybersecurity

Introduction

Modern enterprise environments consist of increasingly complex combinations of networks, endpoints, cloud services, applications, users, and connected devices. As these environments grow, organizations must protect a larger attack surface while cybercriminals continue to develop new methods for exploiting vulnerabilities and avoiding detection. Traditional cybersecurity approaches that rely heavily on periodic security assessments or responding to incidents after they have already occurred may therefore be insufficient. Continuous monitoring provides an alternative approach by allowing organizations to continuously collect and analyze security information in order to identify vulnerabilities and suspicious activity as they emerge.

The Cybersecurity and Infrastructure Security Agency (CISA, n.d.) describes continuous monitoring as an ongoing process of collecting, analyzing, and reporting security information from networks, endpoints, users, and assets. Instead of waiting for a scheduled security assessment, organizations can use this information to maintain visibility into their security posture and respond to emerging threats. However, simply collecting more security information does not necessarily make an organization more secure. The effectiveness of continuous monitoring depends on whether organizations can transform the large amount of information they collect into meaningful and timely security decisions.

This raises an important question: To what extent does continuous monitoring reduce successful cyberattacks and incident response time in an enterprise environment? Evidence from cybersecurity frameworks, academic research, and industry studies suggests that continuous monitoring can significantly improve an organization's ability to detect and respond to cyber threats. By providing centralized visibility, real-time threat detection, automated analysis, and earlier identification of suspicious behavior, continuous monitoring can reduce opportunities for attacks to escalate and shorten incident response time. However, these benefits depend heavily on appropriate security metrics, skilled personnel, effective alert prioritization, automation, and the integration of monitoring technologies with mature incident response processes.

Continuous Monitoring in Enterprise Cybersecurity

Continuous monitoring should not be understood simply as continuously watching network activity. It is a broader cybersecurity risk management process. CISA's Continuous Diagnostics and Mitigation (CDM) Program demonstrates this approach by promoting ongoing collection and analysis of information from networks, endpoints, users, and organizational assets (CISA, n.d.). This continuous visibility allows security teams to identify vulnerabilities, detect unauthorized changes, prioritize risks, and respond to emerging threats more efficiently.

The National Institute of Standards and Technology provides an even broader framework for continuous monitoring. Dempsey et al. (2011) describe Information Security Continuous Monitoring (ISCM) as an important component of an organization's overall risk management strategy. Under this approach, monitoring activities should be connected to an organization's mission, business objectives, and level of acceptable risk. Organizations must determine what should be monitored, how frequently information should be collected, what metrics should be used, and how monitoring results should be communicated to decision-makers.

An important part of the NIST framework is that organizations do not necessarily need to monitor every possible piece of information. Instead, they should identify security metrics that provide useful and actionable information about security controls and organizational risks (Dempsey et al., 2011). Automation can also improve the speed and consistency of monitoring activities, although human oversight remains necessary. Continuous monitoring is therefore better understood as an ongoing process of gathering security information, analyzing it, making decisions based on that information, and responding to identified risks.

How Continuous Monitoring is Implemented

Within an enterprise environment, continuous monitoring is commonly performed through Security Operations Centers (SOCs) and technologies such as Security Information and Event Management (SIEM) systems. Vielberth et al. (2020) identify continuous monitoring, event collection, threat detection, incident analysis, threat intelligence, and coordinated incident response as important functions of modern SOCs. Centralizing these activities allows an organization to combine information from network devices, endpoints, applications, cloud services, and security appliances into a more comprehensive view of its security environment.

SIEM technology plays an important role in creating this centralized visibility. González-Granadillo et al. (2021) explain that SIEM platforms collect and normalize security logs from multiple sources, including firewalls, intrusion detection and prevention systems, antivirus applications, operating systems, network devices, applications, and cloud services. These platforms can then correlate security events, identify suspicious patterns, and generate alerts for security analysts.

Modern SIEM platforms are also increasingly integrated with artificial intelligence, machine learning, threat intelligence, and Security Orchestration, Automation and Response (SOAR) technologies (González-Granadillo et al., 2021). These technologies can help organizations process security information more quickly and automate portions of the detection and response process.

Technology, however, represents only part of an effective monitoring program. The European Union Agency for Cybersecurity (ENISA, 2020) emphasizes the importance of integrating people, processes, and technology. ENISA distinguishes between SOC's, which generally focus on continuous monitoring, detection, and event analysis, and Computer Security Incident Response Teams (CSIRT's), which coordinate incident response, recovery, and communication. This relationship demonstrates why detection alone is not enough. Information produced through monitoring must ultimately result in an effective organizational response.

Continuous Monitoring and Cyber Attack Detection

One of the most important potential benefits of continuous monitoring is early detection. When organizations have limited visibility into their systems, attackers may be able to remain undetected and expand their access before defenders recognize that a compromise has occurred. Continuous monitoring increases the likelihood that suspicious behavior will be identified earlier in the attack process.

The 2025 Verizon Data Breach Investigations Report provides evidence of the importance of detection and visibility in real-world cyber incidents. Verizon (2025) identifies inadequate network visibility, delayed detection, weak credential management, unpatched vulnerabilities, and insufficient monitoring among the weaknesses that can contribute to successful attacks. Delayed detection is particularly dangerous because it can provide attackers with additional time to establish persistence and expand their access before an organization responds.

Continuous monitoring may therefore reduce successful attacks by decreasing the period during which malicious activity can operate unnoticed. This does not mean that monitoring prevents attackers from attempting to compromise systems. Instead, monitoring increases an organization's opportunity to identify suspicious behavior and intervene before an intrusion develops into a more damaging incident.

Artificial intelligence may further improve this capability. Ali et al. (2025) examine the use of artificial intelligence and machine learning for detecting Advanced Persistent Threats in

SOC environments. Their approach incorporated event detection modules and machine-learning algorithms with Splunk and achieved a reported detection accuracy of 99.6%.

More importantly, the approach was designed to reduce false-positive alerts and improve analyst decision-making. By automating portions of alert analysis, security analysts can spend more time investigating genuine threats instead of manually reviewing large numbers of irrelevant alerts.

These findings suggest that the effectiveness of continuous monitoring is influenced not only by the amount of security data collected but also by an organization's ability to accurately analyze that information. Monitoring that produces actionable and accurate alerts provides a greater opportunity for security teams to identify and disrupt attacks before significant damage occurs.

Continuous Monitoring and Incident Response Time

Continuous monitoring may have an even clearer impact on incident response time. Incident response cannot begin effectively until suspicious activity has been detected and communicated to the appropriate personnel. Therefore, reducing the amount of time between the beginning of an incident and its detection can also reduce the overall time required to investigate and contain the incident.

IBM's Cost of a Data Breach Report 2025 provides real-world evidence of this relationship. IBM (2025) reports that organizations with mature monitoring capabilities and security automation generally detect malicious activity sooner, contain incidents more efficiently, and experience lower financial losses than organizations with less mature security operations. Delayed detection, in contrast, allows attackers to remain within systems longer and can increase operational disruption, recovery costs, regulatory exposure, and reputational damage.

Automation can further reduce response time by decreasing the amount of manual work required before analysts can begin investigating genuine threats. SIEM systems can correlate events across multiple security sources, while SOAR and artificial intelligence technologies can assist with alert prioritization and triage. Ali et al. (2025) demonstrate how AI-assisted monitoring can reduce false positives and allow analysts to focus their attention on legitimate threats.

The relationship between monitoring and incident response can therefore be viewed as a chain of activities. Security information must first be collected, suspicious activity must be

identified, alerts must be analyzed and prioritized, and the appropriate response must then be initiated. Improving the speed and accuracy of each step can reduce the time between the beginning of an attack and its containment.

Organizational coordination is also important. ENISA (2020) emphasizes the complementary relationship between SOC and CSIRTs. A SOC may detect suspicious activity, but that detection provides limited value if an organization lacks procedures for escalating the incident and coordinating an appropriate response. Continuous monitoring is therefore most effective when detection capabilities are integrated with established incident response processes.

Measuring the Effectiveness of Continuous Monitoring

Determining whether continuous monitoring actually improves cybersecurity requires organizations to measure its performance. Simply generating more alerts or collecting more logs does not demonstrate that an organization's security has improved.

Forsberg and Frantti (2023) address this issue by proposing a framework for evaluating the technical performance of SOC. They argue that many existing measurements focus on operational factors rather than the actual technical effectiveness of security monitoring. Their framework instead encourages organizations to develop technical metrics that reflect their specific security objectives and environments.

This distinction is particularly important when evaluating the extent to which continuous monitoring reduces successful cyberattacks and incident response time. Organizations could examine factors such as threat detection capability, detection accuracy, false-positive rates, time to detection, investigation time, and containment time. These measurements can help determine whether changes to monitoring technologies or processes are actually producing better security outcomes.

NIST similarly emphasizes the importance of selecting meaningful metrics rather than attempting to monitor everything (Dempsey et al., 2011). The appropriate measurements may vary among organizations because enterprises face different threats, technologies, regulatory requirements, and risk tolerances. Therefore, the effectiveness of continuous monitoring should be evaluated in relation to the security objectives and operational environment of the individual organization.

Limitations et Challenges

Although continuous monitoring provides important cybersecurity benefits, increasing monitoring does not automatically produce better security. One of the most significant problems

is alert fatigue. Modern enterprise security systems can generate extremely large numbers of alerts, many of which may be false positives, duplicates, or low-priority events.

Tariq et al. (2025) explain that excessive alert volume can overwhelm SOC analysts and reduce their ability to investigate threats effectively. Alert fatigue can contribute to delayed investigations, overlooked threats, slower incident response, reduced detection accuracy, analyst burnout, and workforce turnover. This creates a significant problem for continuous monitoring. A system designed to improve detection can become less effective if it produces more information than analysts can reasonably process.

González-Granadillo et al. (2021) identify similar challenges associated with SIEM systems, including false positives, high implementation costs, scalability problems, and the need for skilled analysts. Vielberth et al. (2020) also identify skills shortages, alert overload, increasing attack sophistication, automation limitations, and the lack of standardized performance metrics as continuing challenges for SOCs.

These limitations demonstrate that the quantity of monitoring data is less important than the quality and usefulness of the information produced. Organizations must be able to distinguish important security events from normal activity and low-priority alerts. Alert prioritization, automated triage, contextual threat intelligence, machine learning, and SOAR technologies may help address these challenges (Tariq et al., 2025).

The findings of Ali et al. (2025) provide one possible response to this problem. Their use of machine learning to reduce false-positive alerts suggests that artificial intelligence may help organizations manage the growing amount of information produced by continuous monitoring. Instead of replacing security analysts, these technologies can help analysts concentrate their attention on threats that are more likely to require human investigation.

Conditions for Effective Continuous Monitoring

Taken together, the research suggests that continuous monitoring is most effective when organizations combine appropriate technology with skilled personnel, clearly defined processes, automation, and meaningful performance measurements. Monitoring technology alone cannot guarantee better cybersecurity outcomes.

Organizations require technologies such as SIEM, EDR, intrusion detection and prevention systems, threat intelligence platforms, and increasingly AI-assisted analysis and SOAR. However, these systems must be properly configured and integrated. Organizations must also employ analysts capable of interpreting the information produced by monitoring systems and distinguishing genuine threats from false positives.

Clearly defined workflows are equally important. Security teams must know how alerts should be prioritized, when incidents should be escalated, who is responsible for responding, and how information should move between monitoring and incident response teams. The SOC and CSIRT relationship described by ENISA (2020) demonstrates how monitoring and response must operate together.

Finally, organizations must continuously evaluate their own monitoring performance. Forsberg and Frantti (2023) and Dempsey et al. (2011) both emphasize the importance of meaningful security metrics. By measuring detection accuracy, false-positive rates, detection time, containment time, and other indicators, organizations can identify weaknesses and improve their monitoring strategies over time.

Effective continuous monitoring is therefore not simply continuous data collection. It is a cycle in which organizations collect security information, identify meaningful threats, prioritize those threats, respond to incidents, evaluate performance, and improve the process based on the results.

Conclusion

Continuous monitoring can significantly improve enterprise cybersecurity by increasing visibility into organizational systems, identifying suspicious activity earlier, and allowing security teams to respond more quickly to potential threats. Evidence from NIST, CISA, ENISA, academic research, and industry reports demonstrate that centralized monitoring, SIEM technologies, security automation, and mature SOC operations can strengthen threat detection and improve incident response.

The evidence is particularly strong regarding incident detection and response time. Earlier identification of malicious activity gives security teams an opportunity to investigate and contain incidents before attackers can expand their access or cause additional damage. Industry evidence from IBM and Verizon also demonstrates the operational importance of timely detection and containment.

However, the evidence does not establish that continuous monitoring produces a universal or precise reduction in the percentage of successful cyberattacks. Its effectiveness varies according to the organization's technology, personnel, security processes, metrics, and ability to respond to the information being collected. Excessive monitoring can even become counterproductive when security analysts are overwhelmed by false positives and low-quality alerts.

Therefore, continuous monitoring should not be viewed as a cybersecurity solution by itself. Its greatest value comes from its integration with skilled analysts, appropriate automation, effective incident response procedures, meaningful performance measurements, and continuous improvement. Under these conditions, continuous monitoring can substantially reduce opportunities for attacks to remain undetected, shorten detection and response times, limit the impact of successful intrusions, and strengthen the overall resilience of enterprise cybersecurity operations.

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.
- 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.
- European Union Agency for Cybersecurity. (2020). *How to set up CSIRT and SOC*.
- Forsberg, J., & Frantti, T. (2023). Technical performance metrics of a security operation center. *Computers & Security*, 135, Article 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.
- IBM. (2025). *Cost of a data breach report 2025*.
- 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.
- Verizon. (2025). *2025 data breach investigations report*.

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020). Security operations center: A systematic study and open challenges. *IEEE Access*, 8, 227756–227779.

AI Assisted Outline

I. Introduction

Purpose: Introduce the cybersecurity problem and establish the research question.

- Briefly explain the increasing difficulty enterprises face in detecting attacks across complex networks, endpoints, applications, cloud services, and user activity.
- Explain the problem with relying primarily on periodic assessments or reactive security.
- Introduce continuous monitoring as an approach based on ongoing collection and analysis of security information.
- Establish the two outcomes you are investigating:
 - Reduction in successful cyberattacks
 - Reduction in incident response time
- Research question.

II. Defining Continuous Monitoring in Enterprise Cybersecurity

A. What continuous monitoring means

- Continuous collection of security information
- Analysis and reporting
- Monitoring networks, endpoints, users, assets, vulnerabilities, and security controls
- Difference between continuous monitoring and periodic security assessments

B. Continuous monitoring as risk management

- Explain NIST's Information Security Continuous Monitoring (ISCM) framework.
- Monitoring should align with:
 - organizational mission
 - business objectives
 - risk tolerance
- Organizations should select meaningful security metrics instead of attempting to monitor everything.

C. Automation and human oversight

- Automation improves consistency and timeliness.
- Human judgment remains necessary.

III. How Continuous Monitoring Works in an Enterprise Environment

A. Security Operations Centers (SOCs)

- SOCs as centralized cybersecurity operations
- Continuous event collection
- Threat detection
- Incident analysis
- Threat intelligence
- Coordinated incident response

B. SIEM technology

Explain the role of Security Information and Event Management systems.

- Log collection
- Normalization
- Event correlation
- Real-time monitoring
- Alert generation
- Integration with IDS/IPS, EDR, antivirus, cloud services, etc.

C. SOC and CSIRT coordination

- SOC detects and analyzes suspicious activity.
- CSIRT coordinates incident response, recovery, and communication.
- Monitoring therefore needs to connect detection with actual response procedures.

IV. Impact of Continuous Monitoring on Cyberattack Detection and Prevention

Main sources: Verizon, IBM, Ali et al.

A. Earlier identification of suspicious activity

- Continuous monitoring increases visibility.
- Earlier detection reduces the amount of time attackers can remain unnoticed.
- Monitoring may identify vulnerabilities and suspicious behavior before they escalate.

B. Relationship between delayed detection and successful attacks

Use Verizon to discuss:

- weak visibility
- delayed detection
- insufficient monitoring
- unpatched vulnerabilities
- persistence by attackers
- escalation of compromises

The DBIR material in your bibliography is useful because it connects inadequate visibility and delayed detection with real-world attack patterns rather than only theoretical models.

C. AI-assisted threat detection

Use Ali et al. as a specific example of how monitoring effectiveness can be improved.

- Machine learning
- Automated event detection
- False-positive reduction
- Alert triage
- 99.6% reported detection accuracy in the study
- Allowing analysts to concentrate on genuine threats

V. Impact of Continuous Monitoring on Incident Response Time

A. Faster detection

Explain the basic chain: Continuous data collection → threat identification → alert → investigation → containment → recovery

B. Automation and response

Discuss:

- automated alerting
- automated correlation
- AI-assisted triage
- SOAR
- prioritization
- reduced manual workload

C. Detection and containment

- earlier detection
- faster containment
- reduced breach costs
- improved resilience

D. Organizational coordination

- Detection alone is insufficient.
- Information must reach the appropriate response personnel.
- SOC/CSIRT coordination converts detection into action.

VI. Measuring Whether Continuous Monitoring Is Actually Effective

A. Why measurement matters

- Organizations cannot assume that more alerts equal better security.
- Monitoring effectiveness needs measurable outcomes.

B. Technical performance metrics

Possible measures to discuss:

- detection capability
- detection accuracy
- false-positive rate
- time to detection
- time to investigation
- time to containment
- attack/breach impact

C. Organizational context matters

- No universal metric works equally well for every enterprise.
- Metrics should reflect the organization's risks and objectives.
- Monitoring programs should continuously improve based on measured performance.

VII. Limitations and Challenges of Continuous Monitoring

A. Alert fatigue

- Excessive alert volume
- False positives
- Duplicate alerts
- Low-priority events
- Analyst overload

B. Technology limitations

- Scalability
- Integration
- Implementation costs
- Automation limitations

C. Human and organizational limitations

- Skills shortages
- Poor workflows
- Lack of communication
- Inadequate staffing
- Poorly defined monitoring strategies

D. The paradox of excessive monitoring

More monitoring does not necessarily produce better security.

VIII. Conditions Necessary for Effective Continuous Monitoring

A. Appropriate technologies

- SIEM
- EDR
- IDS/IPS
- Threat intelligence
- SOAR
- AI/ML-assisted analytics

B. Skilled cybersecurity personnel

- Analysts remain necessary despite automation.
- Human oversight and interpretation remain important.

C. Effective processes

- Clearly defined escalation procedures
- SOC/CSIRT coordination
- Incident-response planning
- Continuous improvement

D. Meaningful metrics

- Measure technical performance.
- Evaluate detection accuracy.
- Track response performance.
- Adjust monitoring based on results.

E. High-quality rather than high-volume monitoring

IX. Conclusion

AI Reflection

After picking out my research question and selecting compatible sources, I drafted my own outline before using the assistance of ChatGPT. ChatGPT analyzed my annotated bibliography and suggested an outline based on the sources I had collected. Comparing the two outlines provided a high-level assessment of what was already included, what was missing, and which aspects of the topic were either too broad or too specific. This comparison allowed me to make adjustments without completely changing the direction I originally intended for the paper. It was also useful in organizing the flow of the document in a way that accurately reflected my thought process while making sure that each section logically connected to the next.

Overall, the use of Artificial Intelligence chat helped me cover the necessary aspects of the topic while providing an efficient step-by-step process for presenting my arguments. Instead of replacing my own ideas, it served as a tool for evaluating and organizing them. This made the final paper more focused, helped me identify areas that needed additional support, and allowed me to connect the evidence from my sources more clearly to my thesis and overall research question.

Peer Review Reflection

The peer review process was helpful because both reviewers identified strengths in my research while also pointing out areas where the paper needed further development. Both reviewers agreed that my research question was clear, specific, and relevant to continuous monitoring in enterprise cybersecurity. They also considered the introduction and my discussion of technologies such as EDR, SIEM, and SOAR to be a good foundation. This feedback showed me that I did not need to change the overall direction of my research, but instead needed to better develop and support the ideas that were already included.

One of the most important suggestions was to expand the introduction and better explain why continuous monitoring is important. The reviews helped me realize that explaining the technologies involved was not enough. I also needed to connect faster detection and response to consequences such as financial losses, compromised information, operational disruptions, and damage to an organization's reputation. This made the significance of my research question clearer.

Both reviewers also recommended expanding the Results and Discussion sections. This encouraged me to focus more on what I actually discovered during the research rather than simply describing continuous monitoring. I expanded the discussion of how centralized visibility, automated analysis, and earlier threat detection can reduce incident response time and

limit the impact of successful cyberattacks. I also worked on connecting these findings more directly to my research question.

The second review also pointed out weaknesses in my methodology and suggested explaining how sources were selected and evaluated, including distinguishing between primary and secondary sources. Another useful recommendation was to discuss limitations. This helped me recognize that continuous monitoring should not be presented as automatically improving cybersecurity. Alert fatigue, false positives, differences in organizational resources, skilled personnel, and the quality of monitoring systems can all affect its effectiveness.

Overall, the peer reviews helped me identify areas that made sense to me as the writer but were not developed enough for the reader. Instead of changing my main argument, the feedback helped me strengthen the connections between my research question, evidence, findings, and conclusion. It also encouraged me to present a more balanced argument by discussing both the benefits and limitations of continuous monitoring.

Process Reflection

The research process started with selecting a topic that was both academically relevant and personally interesting to me. I chose to focus on continuous monitoring in enterprise cybersecurity because of my invested interest in the fields of cybersecurity and computer networking. From that interest, I developed a research question that focused on whether continuous monitoring can reduce successful cyberattacks and incident response time within enterprise environments.

Once I established the research question, I began searching academic databases using keywords related to continuous monitoring, incident response, SIEM, SOC operations, cybersecurity monitoring, and threat detection. As I reviewed the search results, I narrowed them down to sources that were credible, relevant, and directly connected to the different aspects of my research question. This process eventually helped me develop my annotated bibliography and better understand the direction of the paper.

Before drafting the paper, I created an organic outline based on how I initially believed the research should be organized. I then compared it with an AI-generated outline based on my annotated bibliography. Comparing the two helped me identify missing areas, improve the organization, and create a more logical progression between ideas.

Finally, the peer reviews provided another perspective by identifying areas that needed additional explanation, stronger methodology, and further development. Together, the research process, outlines, AI assistance, and peer feedback helped shape the final paper into a more organized, focused, and balanced project.