

ENG 211 C 34859

Abdias Noel

August 17, 2026

Proposed Paper Outline (Using Chat GPT)

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