Implementing a Comprehensive Logging, Monitoring, and Auditing Program with Relaxed Access Controls

Leo Newton

10/21/2024

Abstract

This paper outlines a strategy for implementing a comprehensive logging, monitoring, and auditing program in an organization with relaxed access controls. The strategy focuses on leveraging enhanced logging and monitoring capabilities to compensate for the increased risk associated with less restrictive access. It details key events to capture, methods for user monitoring, the importance of baselining, and practical application of auditing tools. This approach aims to maintain a robust security posture despite the inherent challenges of a relaxed access control environment.

Introduction

Organizations sometimes adopt relaxed access controls to foster collaboration and agility. However, this approach increases the risk of security breaches and insider threats. To mitigate these risks, a robust logging, monitoring, and auditing program is essential. This paper presents a strategy for implementing such a program, focusing on capturing crucial events, monitoring user activity, establishing baselines, and utilizing effective auditing tools. This comprehensive approach aims to maintain a strong security posture despite the inherent vulnerabilities of a relaxed access control environment.

Events Captured by Operating System Logs

Operating systems offer a rich source of security-relevant information through their logging capabilities. Critical events that should be captured include:

* Account Logons and Logoffs: Tracking user login and logout times is crucial for identifying unusual activity patterns.
* System Events: These events include system startups and shutdowns, driver installations, and application crashes, which can reveal potential system instability or malicious activity.
* Security Audits: Logs of successful and failed access attempts to resources like files, folders, and registry keys provide insight into potential unauthorized access.
* Object Access: Monitoring attempts to access sensitive files and data objects is essential for detecting unauthorized data exfiltration or modification (Stallings & Brown, 2018).
* Privilege Use: Tracking the use of administrative privileges can help identify potential misuse of elevated permissions.
* Network Connections: Recording network connections, including IP addresses and ports, assists in identifying suspicious network activity.
* Data Modification: Logging changes to critical system files or configurations can help detect tampering or malware infections (Conti et al., 2019).

Monitoring Logged-On Users

Continuous monitoring of logged-on users is crucial in a relaxed access control environment. Key aspects of user monitoring include:

* Real-time Tracking: Implement tools that track user activity in real time, providing immediate alerts for suspicious behavior.
* Session Duration: Monitor the duration of user sessions, flagging unusually long or short sessions that deviate from established baselines.
* Resource Access: Track user access to files, applications, and network resources, noting any attempts to access sensitive data outside of normal job functions.
* Location Monitoring: If feasible, monitor the physical location of logged-on users to detect unauthorized access from unusual locations.

Role of Monitoring in Maintaining a Baseline

Establishing a baseline of normal system and user behavior is fundamental to effective monitoring. A baseline provides a reference point against which to compare current activity, allowing for easier identification of anomalies. Key aspects include:

* Performance Metrics: Establish baselines for CPU usage, memory consumption, and network traffic to identify deviations that could indicate malicious activity.
* User Activity Patterns: Analyze historical user login times, resource access patterns, and data transfer volumes to establish normal behavior profiles (Kim & Solomon, 2019).
* System Events: Track typical system event frequency to identify anomalies such as unexpected reboots or service failures.

Applying Operating System Audit and Logging Tools

Several operating system tools facilitate auditing and logging:

* Windows Event Viewer: This tool provides a centralized interface for viewing and analyzing Windows system logs, including security, application, and system events.
* Linux Auditd: This powerful tool allows for granular configuration of system auditing, enabling the capture of a wide range of events.
* SIEM Solutions: Security Information and Event Management (SIEM) systems aggregate logs from various sources, providing a holistic view of security events and enabling advanced analysis and correlation.

A screenshot of a computer

Description automatically generated

Figure . Windows Event Viewer

Conclusion

Implementing a robust logging, monitoring, and auditing program is essential for maintaining a strong security posture in an environment with relaxed access controls. By capturing key events, monitoring user activity, establishing baselines, and utilizing effective auditing tools, organizations can mitigate the increased risks associated with this approach. This comprehensive strategy ensures that suspicious activities are detected promptly, allowing for swift incident response and minimizing potential damage.

References

Conti, G., Pietrini, R., & Susi, A. (2019). *Intrusion detection systems*. Springer.

Kim, D., & Solomon, M. G. (2019). *Fundamentals of information systems security*. Jones & Bartlett Learning.

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson Education.