Control 8: Audit Log Management (Detailed Explanation with Examples)

Audit log management ensures that all important system activities are recorded, protected, and reviewed. Proper logging helps organizations detect attacks, investigate incidents, and meet legal and compliance requirements.

8.1 Establish and Maintain an Audit Log Management Process

Explanation: Organizations must define a formal logging strategy. This includes deciding which events are logged, who is responsible for reviewing logs, how often reviews occur, and how long logs are stored.

Example: Example: A security policy requires logging authentication failures, administrative actions, and database access. Security staff review these logs every week.

8.2 Collect Audit Logs

Explanation: Logging must be enabled on all enterprise systems, including servers, databases, endpoints, network devices, and applications.

Example: Example: Linux servers log SSH login attempts, Windows systems log account changes, and databases log administrator access.

8.3 Ensure Adequate Audit Log Storage

Explanation: Logs must be stored securely and with enough capacity to prevent loss. Attackers should not be able to delete or modify logs.

Example: Example: Logs are stored on centralized, write-once storage or protected cloud storage with restricted access.

8.4 Standardize Time Synchronization

Explanation: All systems must use synchronized time to ensure events can be accurately correlated during incident investigations.

Example: Example: Firewalls, servers, and SIEM systems use NTP so that an attack timeline is clear.

8.5 Collect Detailed Audit Logs

Explanation: Critical and sensitive systems must collect detailed information to support forensic analysis.

Example: Example: Database logs record username, IP address, timestamp, query executed, and action type.

8.6 Collect DNS Query Audit Logs

Explanation: DNS logs help detect malware communication and suspicious activity by tracking domain requests.

Example: Example: Repeated DNS queries to a known malicious domain trigger a security alert.

8.7 Collect URL Request Audit Logs

Explanation: URL logs record websites accessed by users and systems to detect phishing and data exfiltration.

Example: Example: Logs show a user visiting a fake login page after clicking a phishing email.

8.8 Collect Command-Line Audit Logs

Explanation: Commands executed via PowerShell, Bash, or remote management tools must be logged.

Example: Example: A PowerShell script that downloads malware is recorded in command-line logs.

8.9 Centralize Audit Logs

Explanation: Logs from different systems should be sent to a central platform (SIEM) for correlation and analysis.

Example: Example: Firewall, endpoint, and server logs are sent to an Elastic Stack SIEM.

8.10 Retain Audit Logs

Explanation: Logs must be kept for a defined period based on organizational policy and legal requirements.

Example: Example: Authentication logs are kept for 90 days, while financial logs are stored for 7 years.

8.11 Conduct Audit Log Reviews

Explanation: Organizations must regularly review logs manually or automatically to detect suspicious activity.

Example: Example: A SIEM generates an alert after multiple failed login attempts from a single IP address.

8.12 Collect Service Provider Logs

Explanation: Logs from cloud services and third-party providers must be included for complete visibility.

Example: Example: Cloud provider logs show an administrator login from an unusual geographic location.

Conclusion

Effective audit log management ensures accountability, early detection of cyber threats, accurate incident investigations, and compliance with security standards such as CIS Controls, ISO 27001, and regulatory requirements.