Operating System and Application Logging Guidelines

Regular log collection is critical to ensure security records are stored in sufficient detail for an appropriate period of time. Security logs primarily contain computer security-related information. Operating system and application logs contain a variety of information, including computer security related data.

Implementing the following recommendations will assist in facilitating more efficient and effective log management[1].

At minimum each log event should capture:

- Timestamp (synched to a common time source)
- Event, status and/or error codes
- Service / Command / Application name
- User or system account associated with an event
- Device used (e.g. source and destination IPs, terminal session ID, web browser, etc.)

Log events in an audit logging program should at minimum include[2]:

- Administrative Events
  - Actions taken by any user with root or administrative privileges

- Operating System Events
  - Starting or shutting down of the system
  - Starting or shutting down of a service
  - Network connection changes or failures
  - Changes and attempts to change security settings and controls

- Operating System Audit Records
  - Successful and failed authentication attempts
  - Successful and failed authentication of file access
  - Successful and failed security policy changes
  - Successful and failed account changes (e.g. creation, deletion and privilege assignment)
  - Successful and failed authentication attempts of use of privileges

- Application Account Information
  - Successful and failed authentication attempts
  - Account changes (e.g. creation, deletion and privilege assignment)
  - Use of application privileges

- Application Operations
  - Application actions (e.g. startup, shutdown, success, failures and configuration changes)
  - Application usage (e.g. number of transactions, activity)
  - Application transactions, for example:
    - E-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail
    - Web servers recording each URL requested and the type of response provided
    - Business applications recording financial records were accessed by each user

[1] NIST SP 800-92, Guide to Computer Security Log Management

[2] California State University (CSU) Standard, 8045.S600 Logging Elements