Log review and management

Overview

Purpose:

- How to detect suspicious activities as soon as possible to reduce the impact of incidence or make prevention if possible.
- How to unify the log format and elements as well as the functions?

Role:

- Who typically does this?

Security Administrator or independent party who has no access rights/accounts in the reviewed systems. You can't be an user administrator. At the same time, you review your activity everyday. However, if there is a resource limitation, you need another supervisor to authorize your log review.

Frequency:

It depends on the criticality (i.e. payment system, customer information, business secret, etc.) of the system labelled by the organization, logs could be reviewed ranging from minute, every day, weekly, monthly or even 3 months. In fact, log review is a kind of detective control and the preventive control is lacking. Log review will be the Goal Keeper and frequency is critical.

However, user account and authority list should be reviewed at least 3 to 6 months and never take a check ONLY when the audit cycle is coming

Log Review Tips

Critical systems require at least daily log review, however, what types of logs/activities should we pay attention to?

1. Consecutive login failure especially in non-office hour.

2. Login in non-office hour.

3. Authority change, addition and removal. Check them against with authorized application.

4. Any system administrator's activities

5. Any unknown workstation/server are plugged into the network?

6. Logs removal/log overwritten/log size is full

7. Pay more attention to the log reports after week-end and holiday

8. Any account unlocked/password reset by system administrators without authorized forms?

Log Standard

In fact, we are suffering various log format and standard from various systems even we are working in-house or act

as a consultant. Why don't we produce a standard/guidelines to developer before they design the user administrative and audit trail functions to fulfill security control.

Functions:-

- Search - By date and time, by event type, by criticality, by account/user ID, by department
- Sorting - By date and time, by event type, by criticality, by account/user ID, by department
- Paging (Optional)
- Critical event is marked by "*"
- Log archive and export
- Log code and description table
- Highlighting system and user adminsitrator activities

Mandatory Fields:-

- User ID and Name (Sometimes, event may involve the action from administrator)
- Activity Date/Timestamp
- Activity Code, Type and Description
- Terminal IP address and Location

User Account List:-

- User Info - Name, Department, Role
- Last Accessed Time
- Account Creation Date/Time
- Current Authority and Role
- Account authority and information change history
- Show expired and inactive accounts (for example: 90 days)

Logging Tools

Resources from Syslog.org

- Event Notification

http://www.syslog.org/wiki/Main/EventNotification

- Syslog Clients

http://www.syslog.org/wiki/Main/SyslogClients

- Syslogd Replacements

http://www.syslog.org/wiki/Main/SyslogdReplacements

- Event Viewers

http://www.syslog.org/wiki/Main/EventViewers

- Log Analyzers

http://www.syslog.org/wiki/Main/LogAnalyzers

- Event Correlation

http://www.syslog.org/wiki/Main/EventCorrelation

- Windows

http://www.syslog.org/wiki/Main/Windows

- Misc Log Tools

http://www.syslog.org/wiki/Main/MiscLogTools

Best Practice and Tips from Syslog

- Syslog Security Tip

http://www.syslog.org/wiki/Main/SyslogSecurityTip

- Central Syslog Tip

http://www.syslog.org/wiki/Main/CentralSyslogTip

- Logging Windows To Syslog Server

http://www.syslog.org/wiki/Main/LoggingWindowsToSyslogServer

- Logging Troubleshoot

http://www.syslog.org/wiki/Main/TroubleshootingSyslogForwarding

- Syslog Best Practices

http://www.syslog.org/wiki/Main/SyslogBestPractices

- Logging, Log File Rotation, and Syslog Tutorial

http://www.hccfl.edu/pollock/AUnix2/Logging.htm