File Integration Monitoring (FIM) Security Audit

G. M. Faruk Ahmed, CISSP, CISA, CDCP
www.gmfaruk.com

File Integration Monitoring (FIM) security audit for Windows systems

When performing a File Integration Monitoring security audit for Windows systems, it's important to focus on various files and components to ensure the security and integrity of the system. Here's a list of key files and areas to audit:

1. **File System Security Settings:**

   Audit Policies: Review and audit the security settings related to file access auditing. This can be configured using Group Policy or local security policy settings.

2. **Event Logs:**

   Security Event Log: Examine the Security event log for any suspicious or unauthorized file access, modifications, or deletions.

3. **File Access and Modification Logs:**

   Windows File Auditing: Enable file and folder auditing on critical directories to monitor access and modifications. Use the Security log or specialized audit logs for this purpose.

4. **File Integrity Monitoring Tools:**

   SIEM (Security Information and Event Management) Systems: Monitor alerts generated by SIEM systems for any unexpected file changes.

   Third-party File Integrity Monitoring Tools: Deploy and review logs generated by dedicated file integrity monitoring tools to identify unauthorized changes to files.

5. **System and Security Configuration Files:**

   Security Configuration Baselines: Audit the configuration files that define security baselines for the system. Ensure that they are properly configured and haven't been tampered with.

6. **Antivirus and Antimalware Logs:**

   Antivirus Logs: Check for any detected threats or suspicious activities in the logs of your antivirus and antimalware solutions.

7. **Access Control Lists (ACLs):**

   File and Folder Permissions: Review and audit the permissions and ACLs on critical files and folders. Ensure that only authorized users have the necessary access.

8. **Registry Settings:**

   Registry Security Settings: Review the registry settings related to file access and permissions. Unauthorized changes to these settings can have a significant impact on system security.

9. **Executable Files:**

   System Executables: Monitor and audit critical system executables for unauthorized modifications. Ensure that the digital signatures of these files are valid.

10. **Backup and Restore Logs:**

    Backup Logs: Check logs related to system backups to ensure that they are running successfully and that backup files are secure.

Others Areas:

Group Policy Objects (GPOs):

Group Policy Security Settings: Review GPO settings related to file access and security. Ensure that Group Policies are appropriately configured.

User and Group Management:

User Account Management: Review logs related to user account creation, modification, and deletion. Ensure that only authorized personnel have the ability to make changes.

Network Shares:

Shared Folder Permissions: Review permissions on shared folders to ensure that access is restricted appropriately.

System Logs:

System Event Log: Check the System event log for any hardware or software-related events that may impact file integrity or security.

Critical System Files:

System32 Directory and Critical System Files: Regularly check the integrity of critical system files located in the System32 directory.

Patch Management Logs:

Patch and Update Logs: Ensure that the system is up-to-date with security patches. Review logs related to patch management activities.

Application Logs:

Application-specific Logs: If there are specific applications critical to your environment, review their logs for any file-related security events.

Firewall and Network Security Logs:

Firewall Logs: Examine logs for any unusual network activity that may indicate unauthorized file access or transmission.

To get more content follow me www.gmfaruk.com

LinkedIn: https://www.linkedin.com/in/gmfaruk/

Email: me@gmfaruk.com

File Integration Monitoring (FIM) Security Audit for Linux system

Auditing file integration and monitoring security on a Linux system involves examining various files and configurations to ensure the security of the system. Here are some key files and areas you should consider auditing:

1. **File System Integrity:**
    - /etc/passwd: Check for unauthorized users and ensure that each user has the correct shell and home directory.
    - /etc/shadow: Verify that password hashes are secure and not easily crackable.
    - /etc/group: Ensure that group memberships are appropriate.
    - /etc/sudoers: Review sudo configurations for proper access controls.

2. **System Logs:**
    - /var/log/messages or /var/log/syslog: Look for any suspicious system-wide messages.
    - /var/log/auth.log: Review authentication-related logs for any unauthorized access attempts.

3. **File Permissions:**
    - Use the find command to identify files with unusual or insecure permissions.
    - Check important system binaries and configuration files for unexpected changes in permissions.

4. **Audit Configuration Files:**
    - /etc/audit/auditd.conf: Review and configure the audit daemon settings.
    - /etc/audit/audit.rules: Check the audit rules for monitoring specific system events.

5. **Monitoring Tools Configuration:**
    - /etc/rsyslog.conf or /etc/syslog-ng/syslog-ng.conf: Ensure that logging is configured securely.
    - /etc/logrotate.conf or /etc/logrotate.d/: Verify log rotation configurations.

6. **SSH Configuration:**
    - /etc/ssh/sshd_config: Review SSH server configurations, disable root login, and enforce secure authentication methods.

7. **Firewall Rules:**
    - iptables or firewalld configurations: Ensure that firewall rules are properly configured to restrict unnecessary network traffic.

8. **Intrusion Detection/Prevention Systems:**
    - Review configurations and logs of installed IDS/IPS solutions (e.g., Snort, Suricata).

9. **Filesystem Mount Points:**
    - /etc/fstab: Ensure that only necessary filesystems are mounted, and mount options are secure.

10. **Cron Jobs:**
    - Check crontab entries for all users using crontab -l and inspect files in /etc/cron. directories.

11. **Application-specific Configuration:**
    - Review configurations for specific applications and services running on the system.