4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected (Scored)

Profile Applicability

```
Level 2 - Server
Level 2 - Workstation
```

Description

Monitor SELinux mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or directory.

Rationale

Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Audit

Run the following command and verify output matches:

```
# grep MAC-policy /etc/audit/audit.rules
-w /etc/selinux/ -p wa -k MAC-policy
```

Remediation

Add the following line to the /etc/audit/audit.rules file:

```
-w /etc/selinux/ -p wa -k MAC-policy
```

From:
https://secscan.acron.pl/ - **SecScan**

Permanent link:
https://secscan.acron.pl/centos7/4/1/7

Last update: **2017/05/04 17:05**