1.3.1 Ensure AIDE is installed (Scored)

Profile Applicability

```
Level 1 - Server
Level 1 - Workstation
```

Description

AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system.

Rationale

By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Audit

Run the following command and verify AIDE is installed:

```
# dpkg -s aide
```

Remediation

Run the following command to install AIDE:

```
# apt-get install aide
```

Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

Initialize AIDE:

```
# aide --init
```

Reference

AIDE stable manual: http://aide.sourceforge.net/stable/manual.html

Notes

The prelinking feature can interfere with AIDE because it alters binaries to speed up their start up times. Run `prelink -ua` to restore the binaries to their prelinked state, thus avoiding false positives from AIDE.