CCDC Inject

INJECT NAME	Solution to Monitor File System Integrity
INJECT ID	SOCS01A

INJECT DESCRIPTION:
There is considerable concern about key files being tampered with and going undetected for long periods, as a result of hackers or simply mistakes. Develop a set of tools that will provide for the monitoring of a directory of files and placing alerts in SYSLOG should any files be found to be different from an initial snapshot.

Two tools will need to be developed. First is a took that takes all the files in a directory and snapshots their current fingerprint (perhaps a hash code and file size). A second tool would run as a CRON/AT job every 5 minutes to monitor that directory and detect any files that were different from the snapshot. There would be a unique job for every directory that needed to be monitored.

Create these tools for both Windows and Linux.

INJECT DELIVERABLE
Prepare a clearly written memo that provides the code for each script with reasonable comments to describe the key sections of code. Provide screen shots of the script creating the snapshot information on a Linux and Windows server and the monitoring code running and detecting a changed file. Use screenshots for evidence of functionality.