**Use Case: Notify system administrator of a potentially unwanted change to a system file**

**Iteration:** 1

**Primary Actor:**  Corporate System Administrator

**Goal in Context:** To detect and alert a system administrator of a potentially undesired change in a protected file on an employee’s machine.

**Preconditions:** Base Image must becreated for comparison, e-mail address to which to send notification must be setup, program must be active on target machine.

**Trigger:** The change is detected during a scheduled scan.

**Scenario:**

1. An employee, either accidentally or intentionally, installs spyware on their company machine that creates an autostart registry key and sends information gathered from the network (usernames, passwords, account info, vulnerabilities, etc.) to an e-mail address.
2. During a regularly scheduled scan, the program computes a hash code for the infected file and compares it to the code stored for that file in the base image.
3. Finding that the codes do not match, a log entry is generated including the affected machine’s name, file name and path of affected file, time the file was changed, the time of the scan, and the username of the account changing the file.
4. Unless a setting says otherwise, an alert message displaying the new log entry is displayed on the machine.
5. An e-mail is generated and sent to the specified system administrator’s account containing the log entry.

**Exceptions:**

1. Registered notification e-mail address is invalid.
2. Network connectivity issue prevents e-mail from being sent.

**Priority:**  High, to be implemented as a basic feature

**When Available:** Second increment

**Frequency of Use:** High frequency depending on scanning schedule

**Channel to Actor:** Log file, e-mail notification

**Secondary Actors:** Employee

**Channels to Secondary Actors:** Screen output

**Open Issues:**

1. How can this process be adapted to real time?