Operating system security

Record all initial setup of list of process as blue print and checksum to compare difference in future audit

Record all the time taken by each process and threads as audit shown in log to review every day and compare with initial setup record and ask authorisation before adding new process to the list to run or kill process and thread. Check all the checksum of each process before run or kill process.

Every 3 minutes to kill non-operating system process and threads and not allow restart process or thread in 2 minutes after kill

Record any retry to restart the process and thread’s program to get authorised before restart.

Banker algorithm is used

Preempt algorithm is used

Bonus: Remove read right from files and write files with append and no need to read file when write file to provide ultimate security, can it insert after append and save file by organising file bits without read operation

Bonus: docker each process and use random file names in system and encryption data in use read operation without decrypt by CPU, even CPU also see data in encrypted or Two CPU, CPU 1 read first bit and CPU 2 read second bit.

Ultimate Bonus: memory address randomisation that malware can not know where to start and insert and run.

Ultimate Bonus: No process format and No File format, malware can not know where to start and insert and run. Length of border of process and files unknown and inexist format are random

Remark: Operating system is a program to allow create another operating system like program by using isolation to secure each process.