Kickstart: SIEM and Log Analysis

This material is prepared for use in *SIEM and Log Analysis course* and was prepared by Henrik Kramselund Jereminsen, http://www.zencurity.com . It contains the very basic information to get started!

These course and exercises are expected to be performed in a training setting with network connected systems. The exercises use a number of tools which can be copied and reused after training. A lot is described about setting up your workstation in the Github repositories.

The main site is: https://github.com/kramse/

I try to gather all information there!

So to get kickstarted in this course:

- ☐ Make sure you can login to Fronter
  https://kea-fronter.itslearning.com/
  Electronic version of this document will be uploaded here!
- ☐ Bookmark the main Github page: https://github.com/kramse/
  Note: there are two pinned repositories `security-courses` and `kramse-labs`
- ☐ Lecture plan for this course
  https://zencurity.gitbook.io/kea-it-sikkerhed/siem-and-log-analysis/lektionsplan
  (Source is also in Git https://github.com/kramse/kea-it-sikkerhed)
- ☐ Slides and exercises booklet – clone or download single files
  https://github.com/kramse/security-courses/tree/master/courses/system-and-software/siem-log-analysis
- ☐ Read about setup of exercise systems here
  https://github.com/kramse/kramse-labs
- ☐ Check BIOS settings - make sure CPU settings have virtualisation turned ON
- ☐ Select and install virtualisation software
- ☐ Get the books! Either on paper or PDF

I hope we will have a fun and enjoyable time in this course.