# Minute

1. Content

* Report: Alert correlation survey: framework and techniques
  + Papers need to be read for each module
    - Normalization
      * [7]
    - Aggregation
      * [12]
      * [4]
    - Correlation
      * [3]
      * MIRADOR
      * LAMDA
      * JIGSAW
    - False Alert reduction
      * [21] vs [36]
      * [35]
      * [37]
    - Attack strategy analysis
      * [20]
      * [25]
    - Prioritization
      * [22]
      * [18]

Note: these reference numbers are based on “Alert correlation survey: framework and techniques” references.

* Schedule for each member: each member should have a schedule for himself.

1. Tasks

* Find and read paper [7]
* How to convert from XML(IDMEF) to predicates ?
  + Find paper(s) which address(es) this problem. Deadline: 24h 19/9/2010
  + Read this paper

1. Group rules
   1. All paper report must be in Vietnamese.