Minutes

1. Content:

* Discussing about IDMEF, how to convert IDMEF to predicate.
* Problems about pre-post approach, how to construct hyper-alert type.

1. Tasks:

* Reading about host-based IDS.
* Send mail to some authors of papers which used pre-post approach.
* Modify the concrete architecture, the output of Normalization is IDMEF.
* Find papers about creating predicates after aggregation of raw alerts.