Towards Self Adaptable Security Monitoring in IaaS clouds

Anna Giannakou, Louis Rilling, Jean-Louis Pazat, Frederic Majorczyk, Christine Morin
The need for adaptable security monitoring

- IaaS cloud environments are very dynamic
  - Topology related changes (VM creation, deletion, migration)
  - Traffic load fluctuation
  - Service addition/removal
  - Traditional security monitoring is ineffective
  - Reconfiguration of monitoring system should be automated

- Several actors with different security requirements
  - Tenants express their requirements through SLA
Self adaptable security monitoring engine - SAIDS(1)
Self adaptable security monitoring engine- SAIDS(2)
Self adaptable security monitoring engine - SAIDS(3)
Self adaptable security monitoring engine - SAIDS(4)
Self adaptable security monitoring engine - SAIDS(5)
Conclusion & Future work

**Conclusion:**
- Environmental changes affect the effectiveness of a traditional security monitoring architecture in the cloud
- Automatic reconfiguration is necessary

**Future work:**
- Include other security devices (ex. Firewalls)
- Aggregate logs from various locations
- Address multi-tenancy