Self Adaptation for Security Monitoring in IaaS clouds
Anna Giannakou, Louis Rilling, Christine Morin, Jean-Louis Pazat

To cite this version:

HAL Id: hal-01340460
https://inria.hal.science/hal-01340460
Submitted on 1 Jul 2016
Self Adaptation for Security Monitoring in IaaS clouds

Anna Giannakou*, Louis Rilling®, Christine Morin*, Jean-Louis Pazat*
* Inria, ®DGA

**Context:** IaaS cloud environments.
Frequent infrastructure-related changes:
- VM creation, migration, destruction
- Service addition or removal

**Problem:** Frequent changes make traditional security monitoring fail

**Related work:** Projects that partially address tenant driven customization and scalability issues [1][2] but fail to adapt to frequent changes. [3] addresses self-adaptation but not multi-tenancy, tenant-driven customization or cost-effectiveness.

**Objectives**
- **Self adaptability:** react to changes in virtual and physical infrastructures
- **Customization:** allow tenants to request detection of specific types of attacks
- **Scalability:** adapt to traffic load and changes in the size of the infrastructure
- **Cost minimization:** for tenants and the provider

**SAIDS Features**
- **Adaptation probes:** detect a change and reconfigure the components involved
- **Customized rules:** include IDS rules targeting a tenant’s deployed services
- **New sensor deployment:** rebalance traffic analysis when a local intrusion detection sensor is overloaded
- **Component sharing:** tenants may share local IDS sensors

**SAIDS architecture**

1. **Infrastructure monitoring probes** notify the adaptation manager that a topology change occurs and relate the necessary information: VM id, VM IP, hostname of physical host
2. **Adaptation manager** decides which additional rules have to be activated in the **local IDS** (IIDS) responsible for the new host of the VM. Decision based on:
   - Deployed services (VM info)
   - Specific requests from tenants (SLA info)
3. The adaptation manager adapts the IIDS through remote execution of the adaptation driver

**Early evaluation**

**Goals**
Evaluating the reconfiguration overhead & quality of detection

**Technologies**
- Cloud deployed with Openstack
- Inter VM communication through GRE tunnels on Open vSwitch

**Scenario**
- Load balanced setup representative of a production env.
- 3 interconnected VMs: web, mail, DNS services
- 2 IIDSs: one per virtual switch

**Future Work**
- Combine monitoring for provider and tenants
- Add other devices: collectors, aggregators
- Offer tenants partial control of the framework

**Results**

- **Time in secs**
  - Without adaptation: 2.3
  - With adaptation: 1.7

- **Options**

---

**Figure:** Diagram illustrating the SAIDS architecture and its components, including the flow of information and decision-making processes. The diagram integrates elements such as rule update manager, adaptation driver, rule repo, IIDS, adaptation manager, infrastructure monitoring probe, and cloud controller.