Sniff Hynesim

IETA RIGAUD Michaël

ENSTA Bretagne

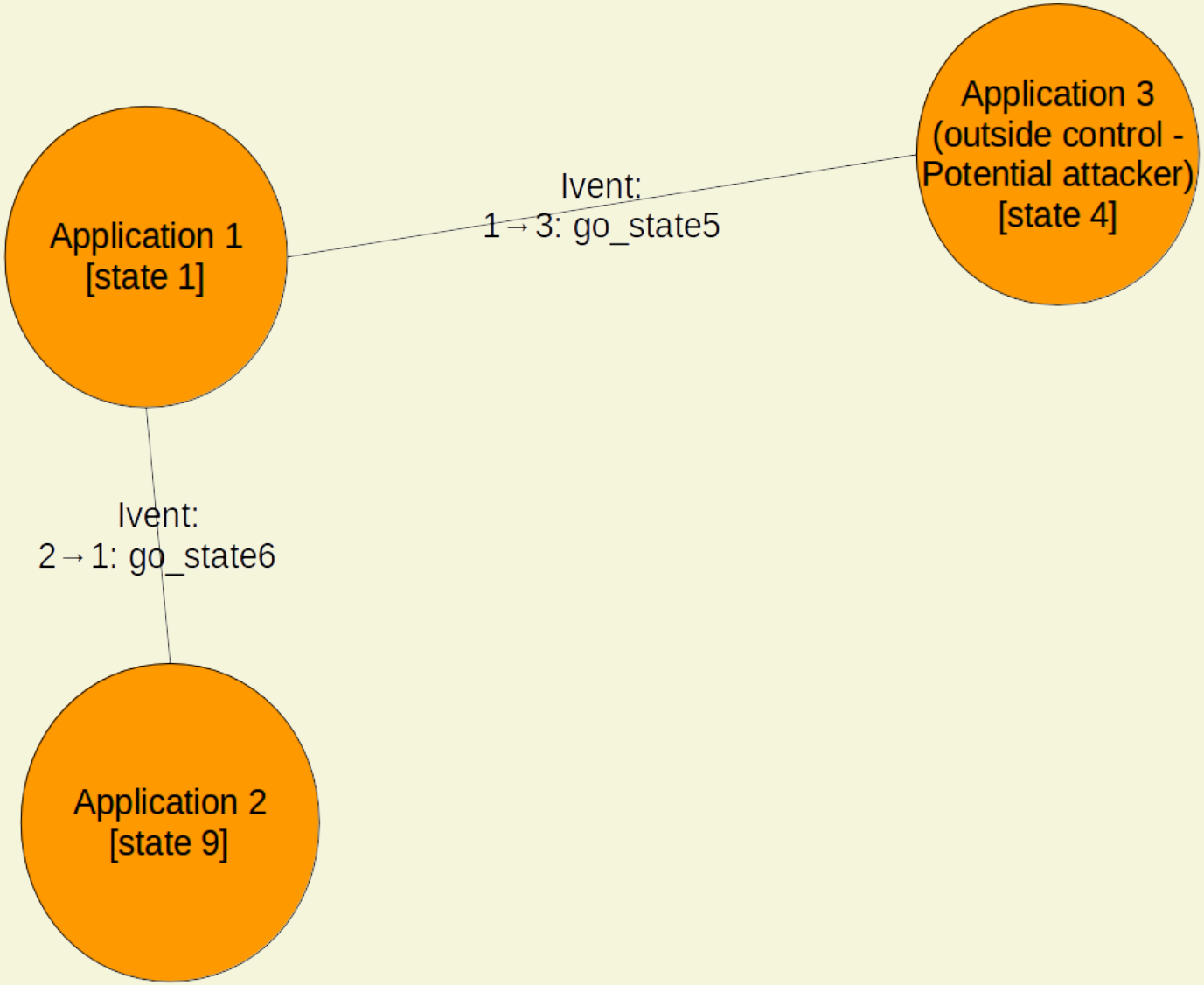
13 mars 2017

Sommaire

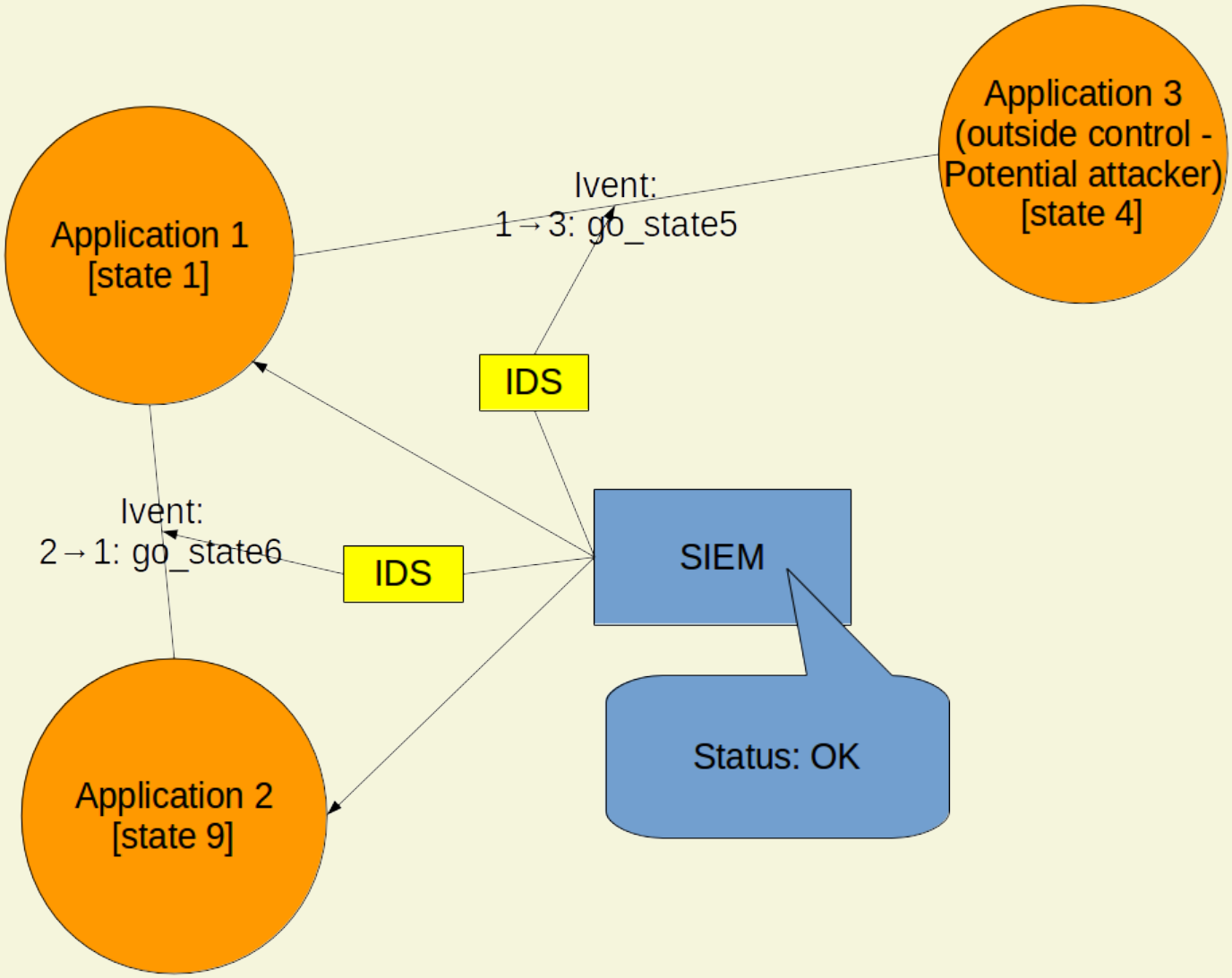
Introduction

Sommaire

Aim of the project



Technical choices



Organization

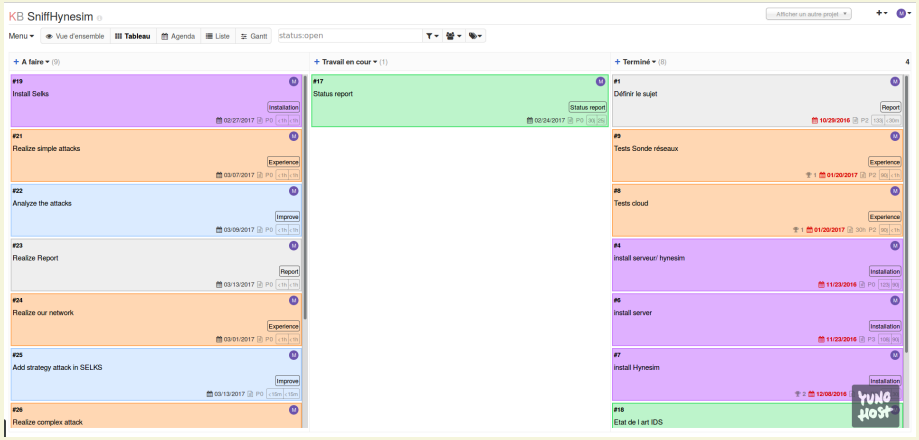


FIGURE – Kanban

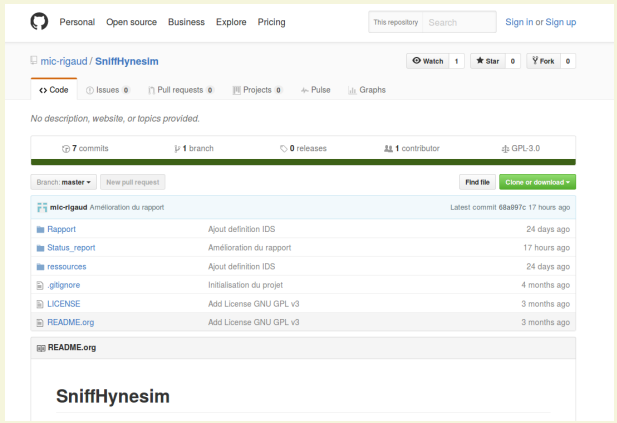


FIGURE – Github

Sommaire

Installation

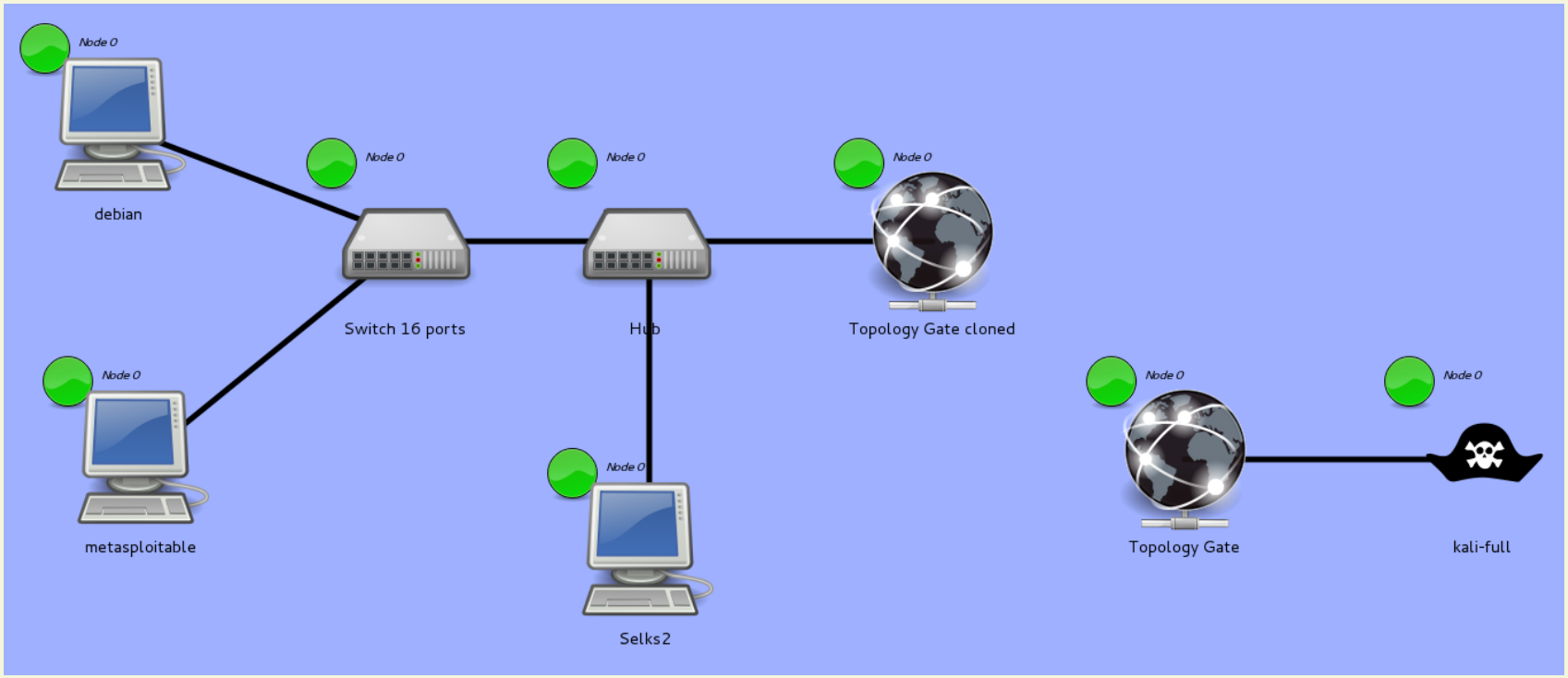
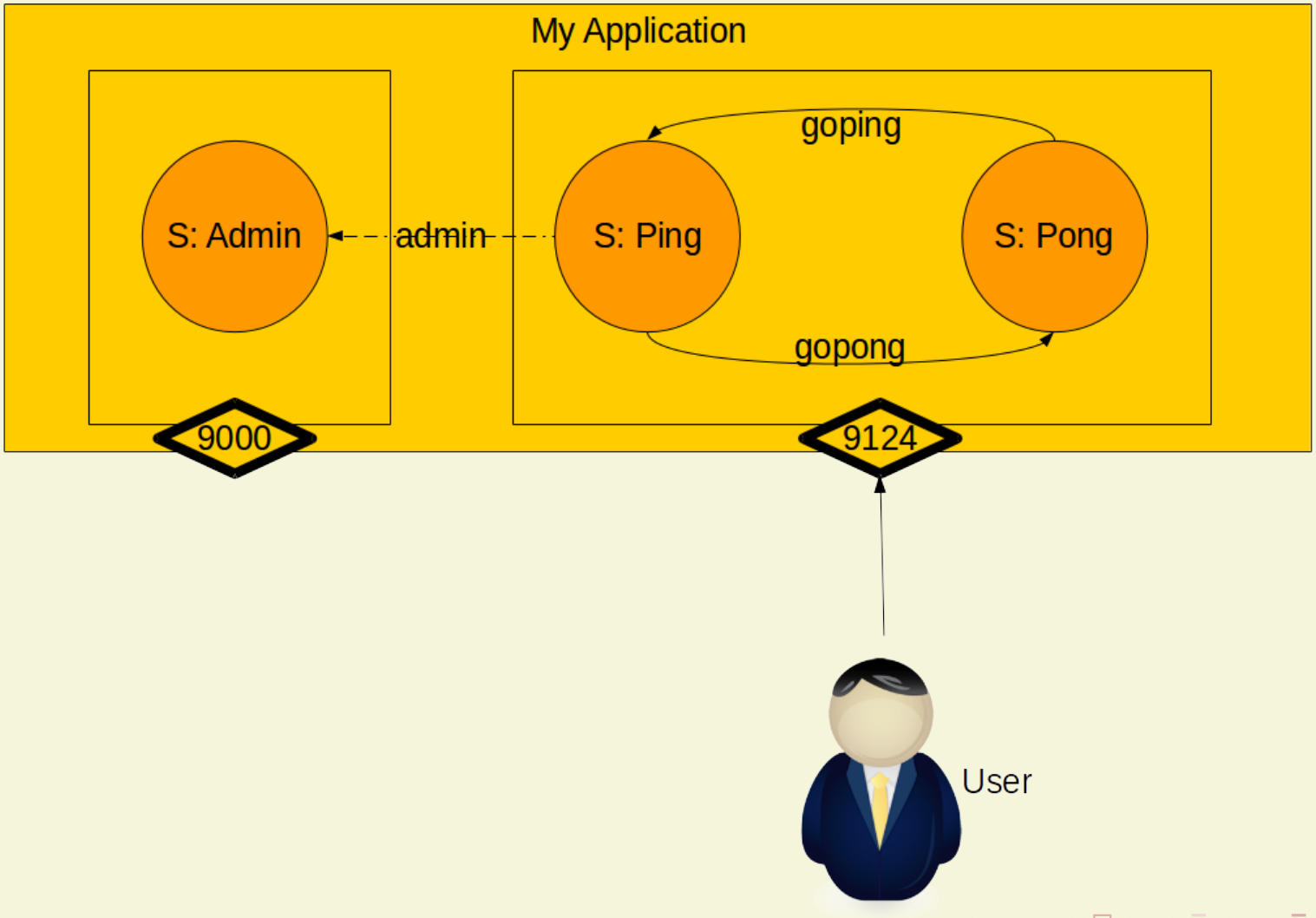
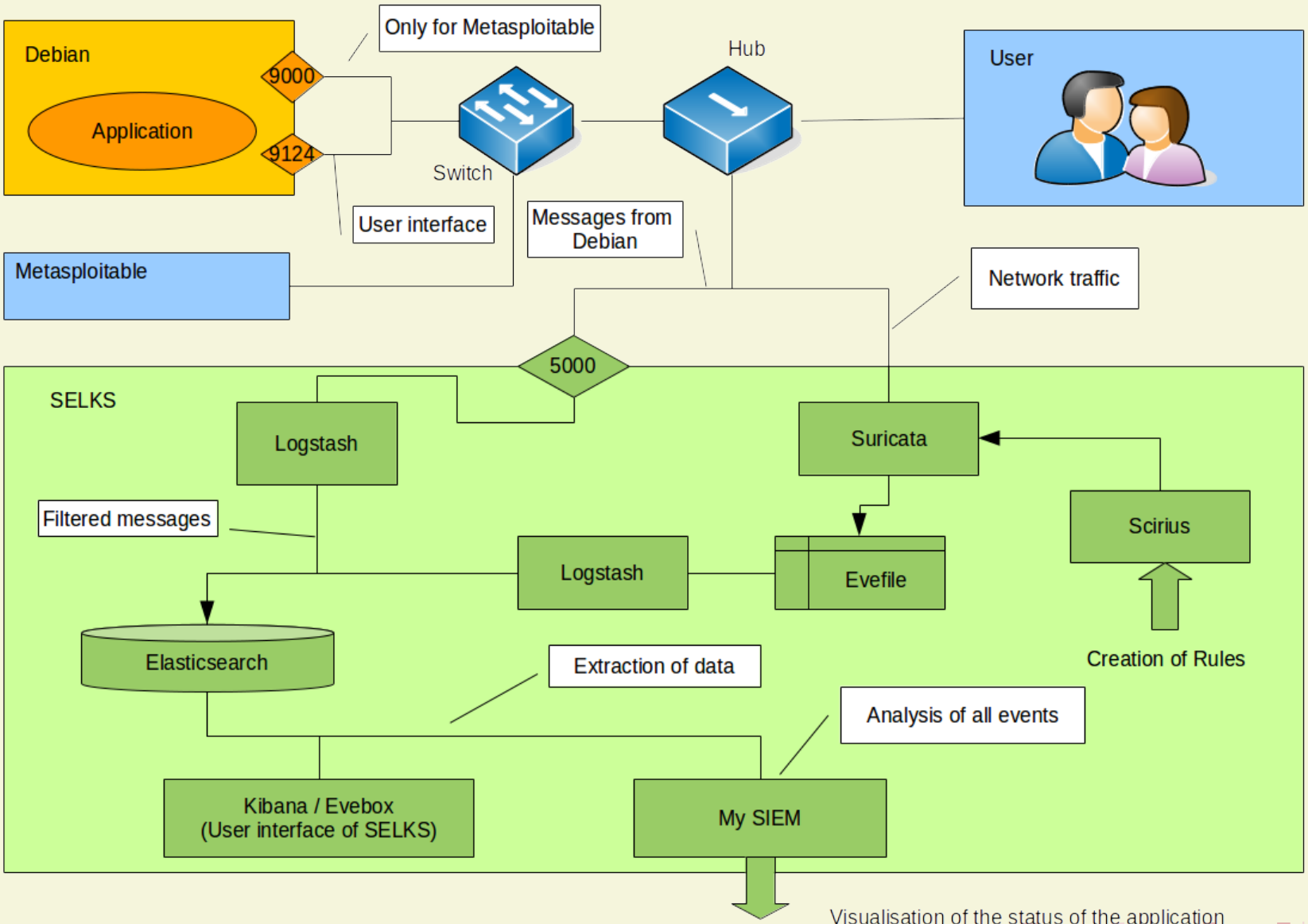


FIGURE – Network installed

Application



Detection system



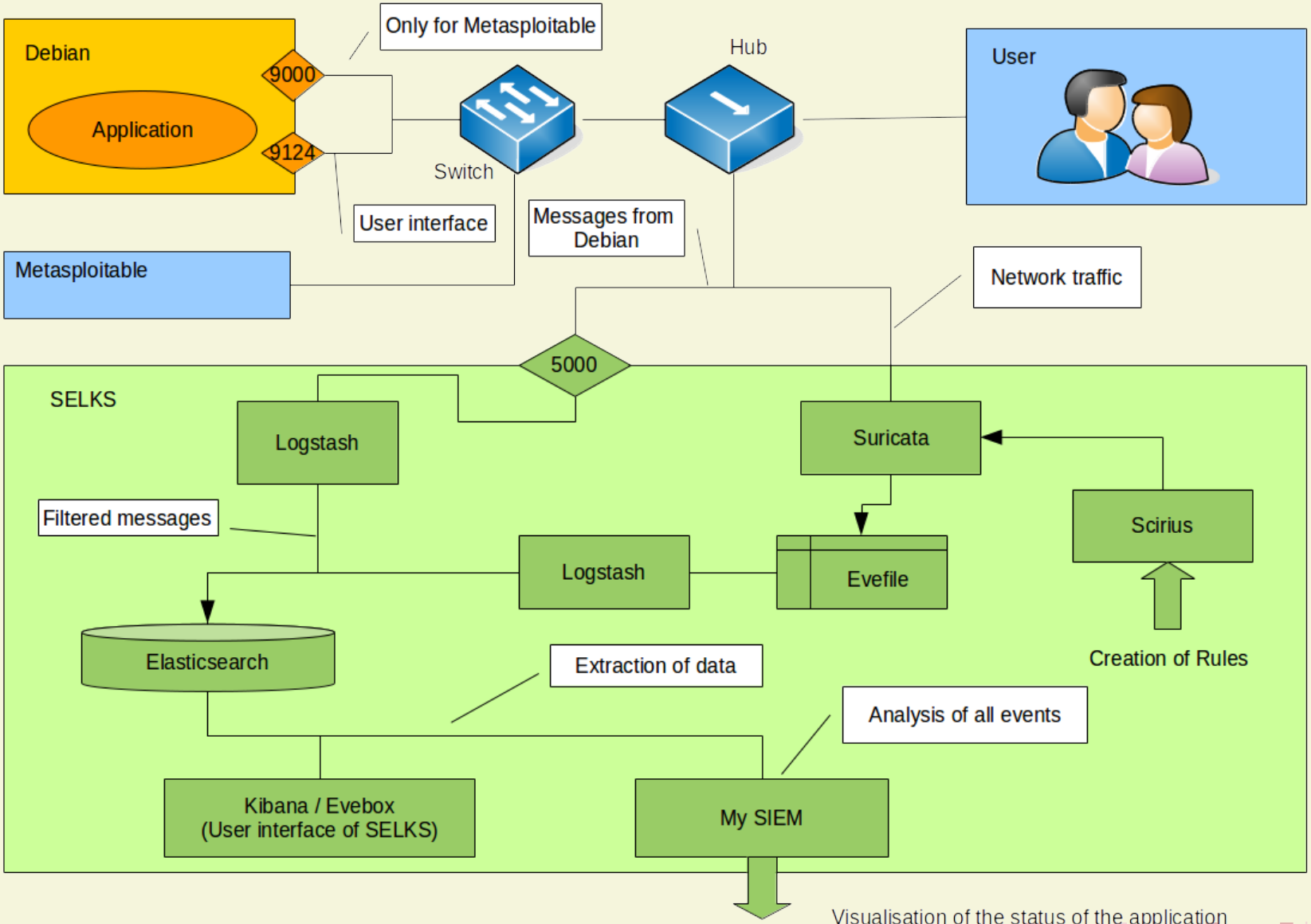
Sommaire

Results

Way of improvements

Sommaire

Conclusion


Debian
9000
Application
9124
Only for Metasploitable
Switch
Hub
User
User interface
Messages from Debian
Metasploitable
Network traffic
5000
SELKS
Logstash
Suricata
Filtered messages
Scirius
Logstash
Evefile
Elasticsearch
Creation of Rules
Extraction of data
Analysis of all events
Kibana / Evebox
(User interface of SELKS)
My SIEM
Visualisation of the status of the application

Demonstration

Bibliography

[1] 3ilson.org. Selks + esxi installation guide. Youtube, October 2016.

[2] Vangie Beal. intrusion detection system. Webopedia.

[3] Diateam. Hynesim. https ://www.hynesim.org/.

[4] Solange Ghernaouti. *Sécurité informatique et réseaux*, volume 4, chapter 8.4. Dunod, 2013. At Ensta Bretagne code : I11 GHE.

[5] Frédéric Guillot. Kanboard. https ://kanboard.net/.

[6] Jonathan Krier. Les systèmes de détection d'intrusions. Technical report, developpez.com, july 2006.

[7] Eric Leblond. Let's talk about selks. In *SSTIC conference*, June 2014.

[8] Eric Leblond. Suricata, dévoilez la face sécurité de votre réseau. *Gnu Linux Magazine France Hors-série*, 76 :9, 2015.

[9] David Peterson. What is kanban. Technical report, KanbanBlog, 2009.

[10] StamusNetworks. Selks. `https://github.com/StamusNetworks/SELKS`, 2014.

[11] wikipedia. Security information and event management, 2017.

Questions ?

IDS

Definition 6.1 : *IDS*

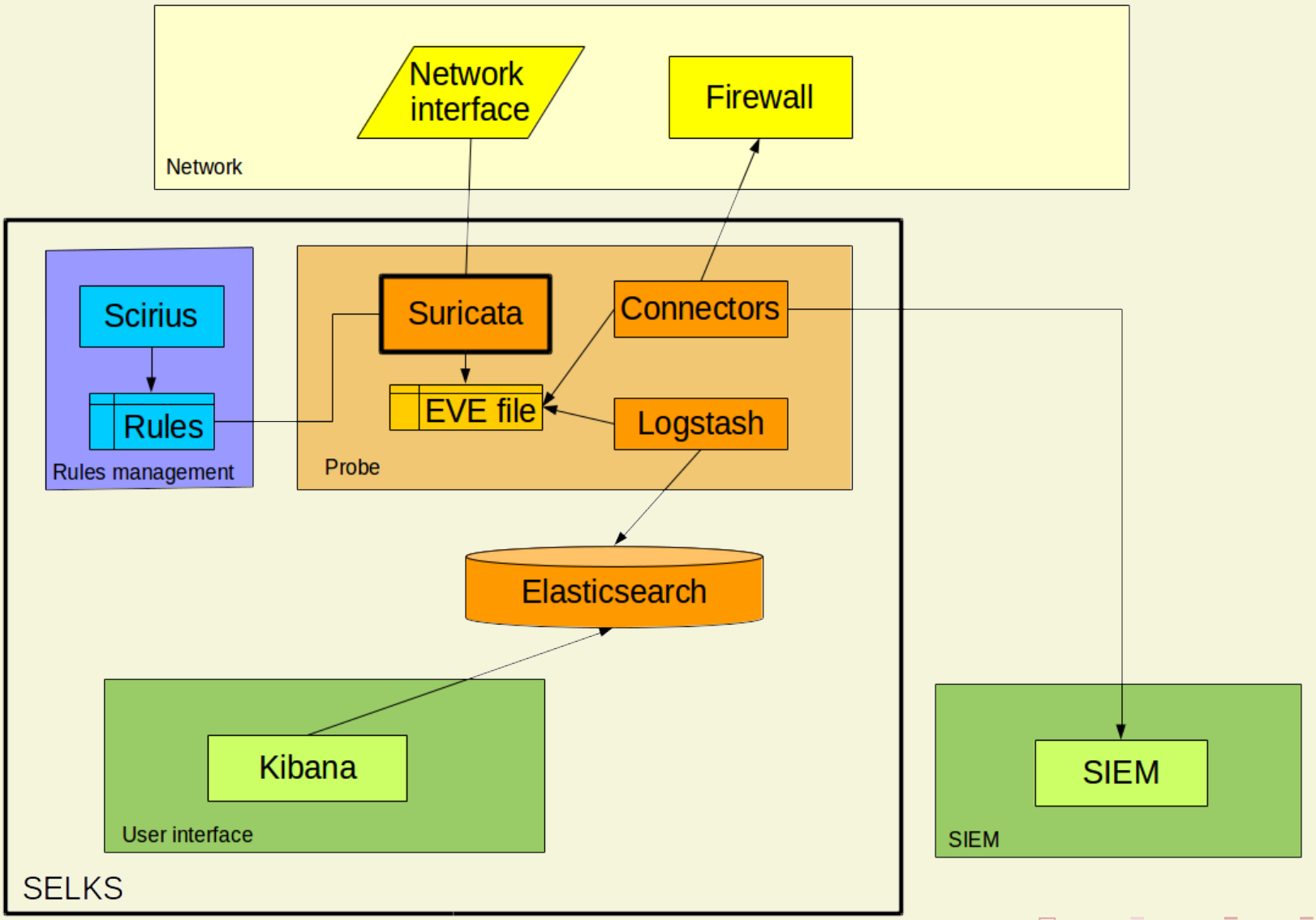
An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

SIEM

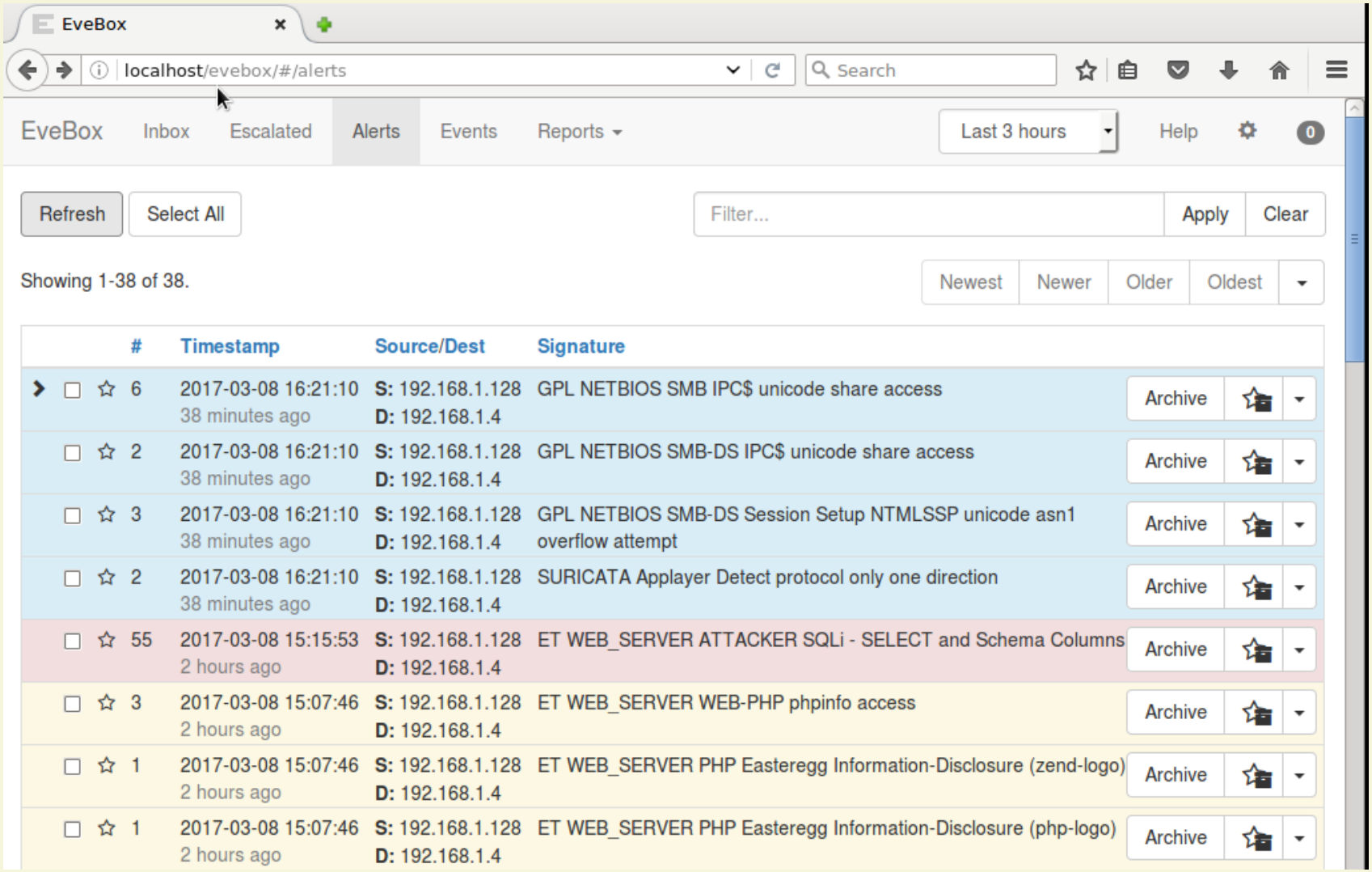
Definition 6.2 : *SIEM*

In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by network hardware and applications.

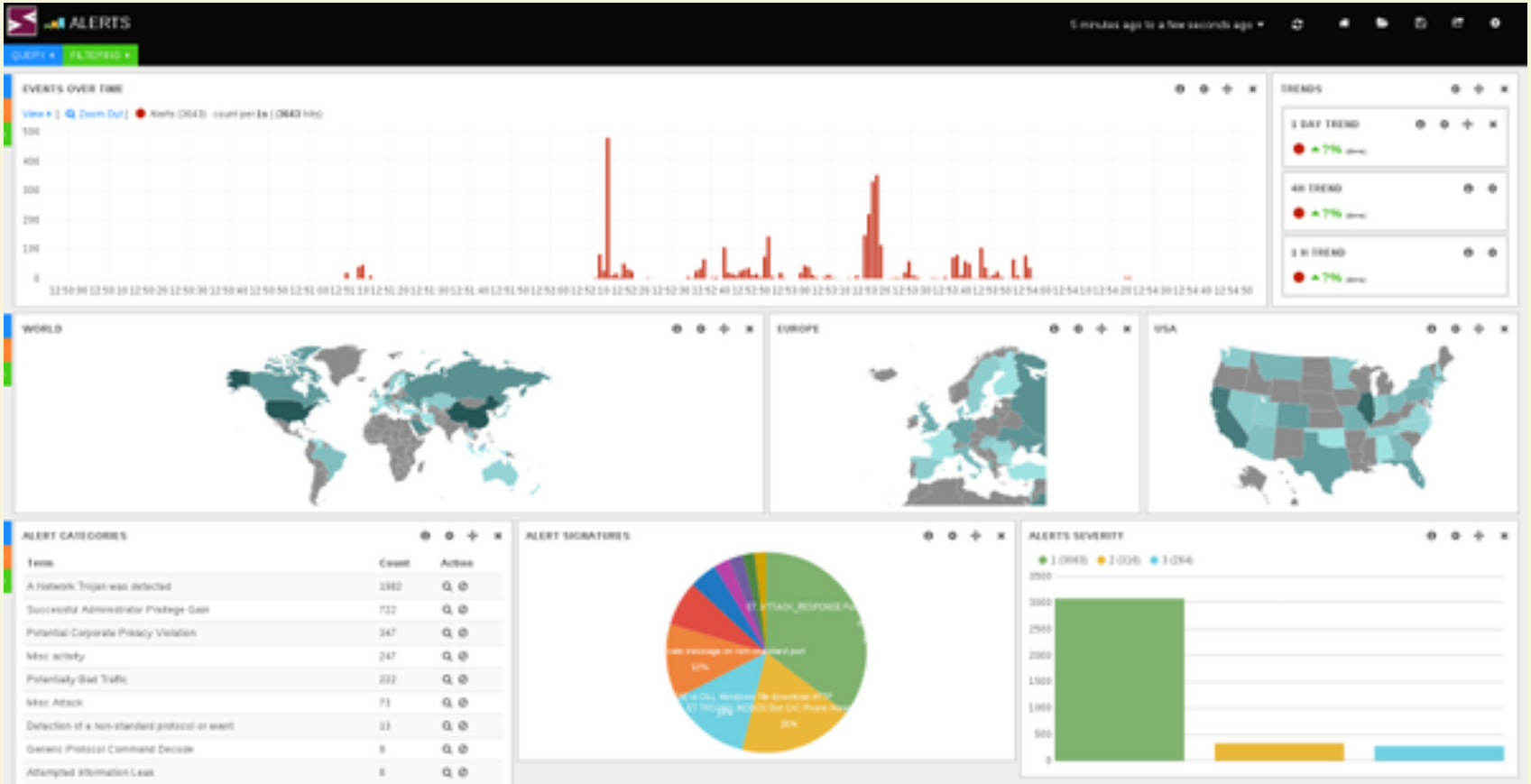
SELKS


Network
Network interface
Firewall
Scirius
Rules
Rules management
Suricata
EVE file
Probe
Connectors
Logstash
Elasticsearch
Kibana
User interface
SELKS
SIEM
SIEM

Evebox


EveBox
localhost/evebox/#/alerts
Search
EveBox
Inbox
Escalated
Alerts
Events
Reports
Last 3 hours
Help
0
Refresh
Select All
Filter...
Apply
Clear
Showing 1-38 of 38.
Newest
Newer
Older
Oldest
Timestamp Source/Dest Signature
6 2017-03-08 16:21:10 38 minutes ago S: 192.168.1.128 D: 192.168.1.4 GPL NETBIOS SMB IPC$ unicode share access Archive
2 2017-03-08 16:21:10 38 minutes ago S: 192.168.1.128 D: 192.168.1.4 GPL NETBIOS SMB-DS IPC$ unicode share access Archive
3 2017-03-08 16:21:10 38 minutes ago S: 192.168.1.128 D: 192.168.1.4 GPL NETBIOS SMB-DS Session Setup NTMLSSP unicode asn1 overflow attempt Archive
2 2017-03-08 16:21:10 38 minutes ago S: 192.168.1.128 D: 192.168.1.4 SURICATA Applayer Detect protocol only one direction Archive
55 2017-03-08 15:15:53 2 hours ago S: 192.168.1.128 D: 192.168.1.4 ET WEB_SERVER ATTACKER SQLi - SELECT and Schema Columns Archive
3 2017-03-08 15:07:46 2 hours ago S: 192.168.1.128 D: 192.168.1.4 ET WEB_SERVER WEB-PHP phpinfo access Archive
1 2017-03-08 15:07:46 2 hours ago S: 192.168.1.128 D: 192.168.1.4 ET WEB_SERVER PHP Easteregg Information-Disclosure (zend-logo) Archive
1 2017-03-08 15:07:46 2 hours ago S: 192.168.1.128 D: 192.168.1.4 ET WEB_SERVER PHP Easteregg Information-Disclosure (php-logo) Archive

Kibana


ALERTS
EVENTS OVER TIME
TRENDS
WORLD
EUROPE
USA
ALERT CATEGORIES
ALERT SIGNATURES
ALERTS SEVERITY

IDS rules

```
alert tcp any any -> any 9124 (msg:"Action goping"; \
content:"goping"; sid:501; rev:5000;)

alert tcp any any -> any 9124 (msg:"Action gopong"; \
content:"gopong"; sid:502; rev:5001;)

alert tcp any any -> any 9000 (msg:"Connexion vers l interface admin"; \
flow:established,to_server sid:504; rev:5002;)
```

SIEM : Application probe

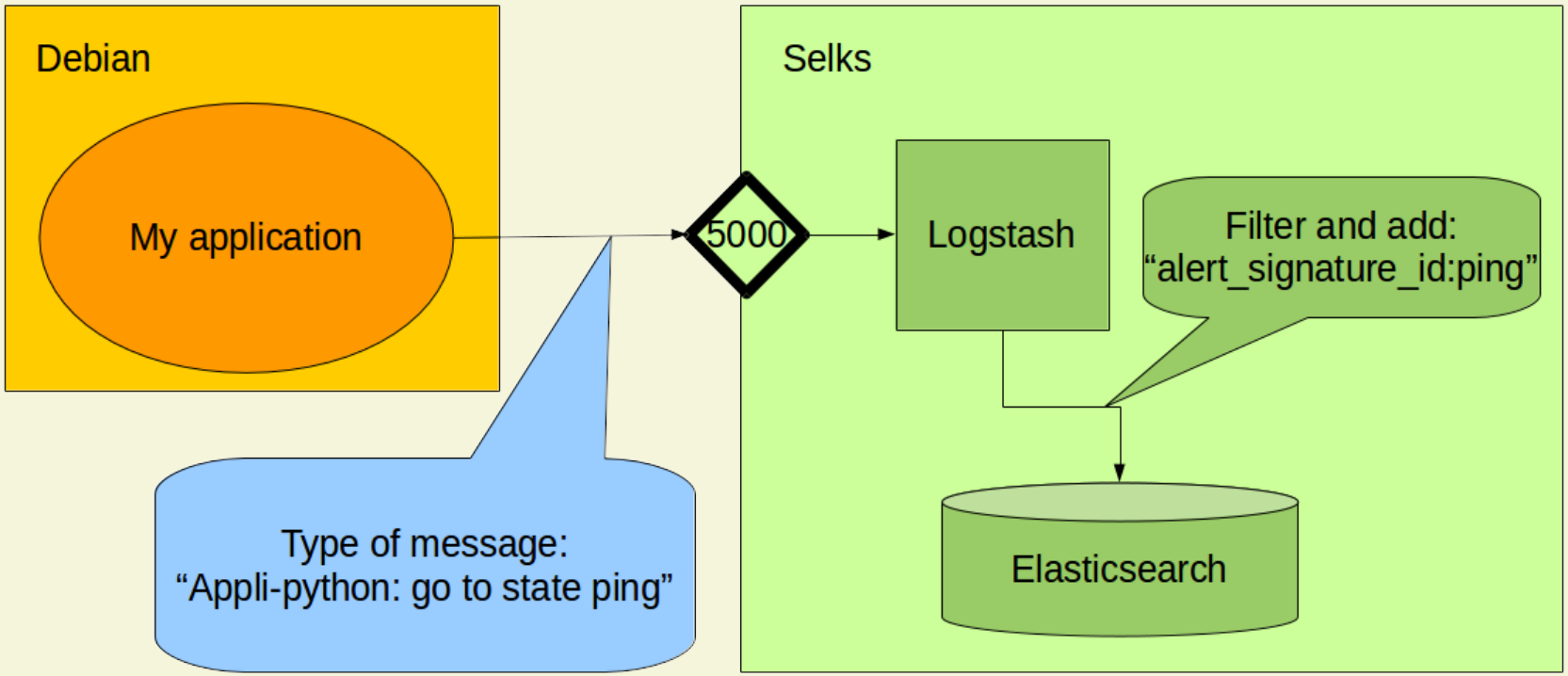


FIGURE – Data processing

SIEM : Implementation

```
root@SELKS:~/Documents/SIEM# ./main.py
##########################################################
                SIEM DEVELOPPE PAR MICHAEL
              Application sous license GPLV2
##########################################################

App-status: Ping  |  Net-status: Admin  |  Attaque: True

##########################################################
root@SELKS:~/Documents/SIEM#
```

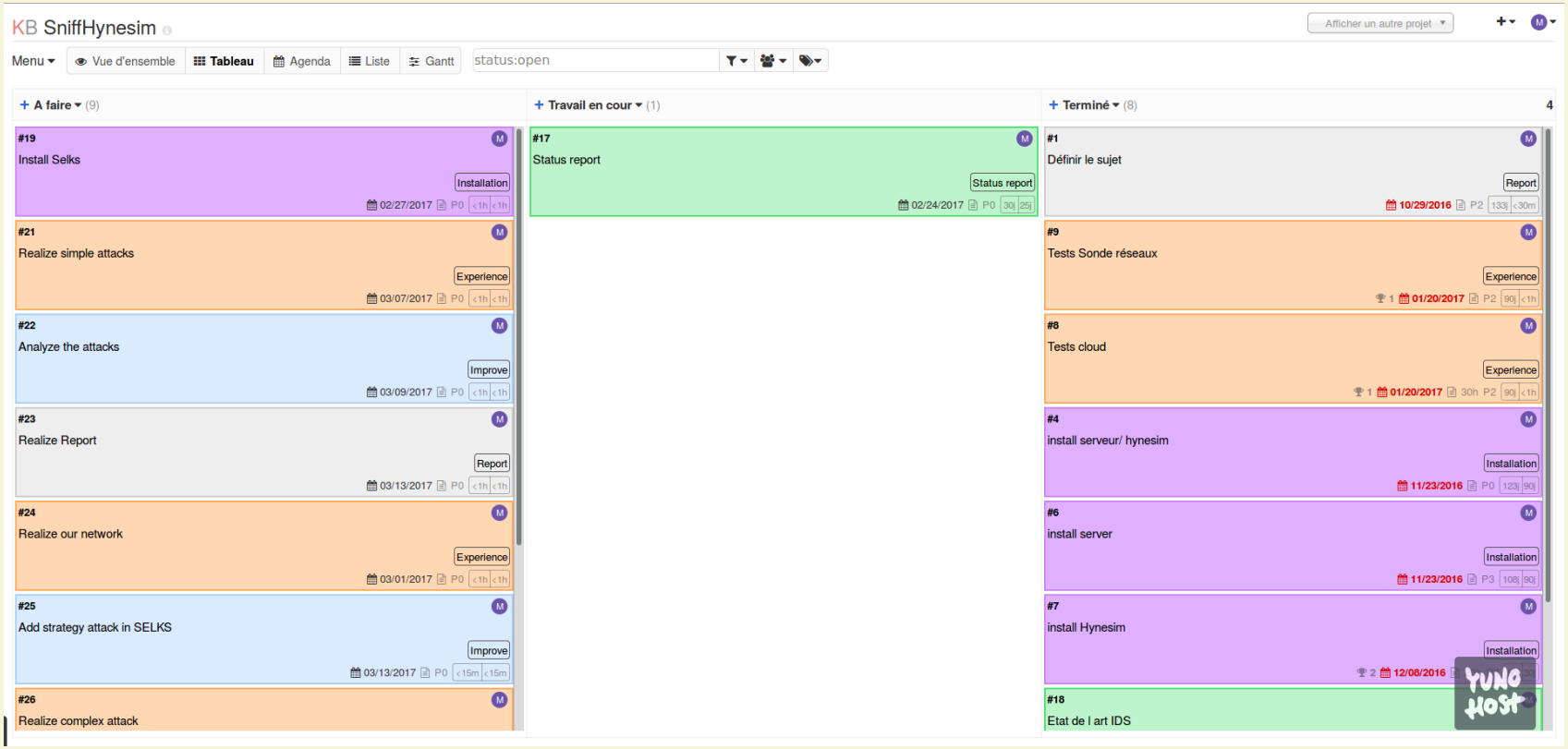
FIGURE – My SIEM

Kanban : Definition

Definition 6.3 : *Kanban*

Kanban is a new technique for managing a software development process in a highly efficient way. Kanban underpins Toyota's "just-in-time" (JIT) production system. The kanban system consists of a big board on the wall with cards or sticky notes placed in columns with numbers at the top

Kanban : kanboard



https://mic-rigaud.fr/kanboard/?controller=BoardViewController&action=readonly&token=10ea65eca908023dbcd8bc8dce75791c7a14d67912627dafaa5b1003