Sniff Hynesim

IETA RIGAUD Michaël

ENSTA Bretagne

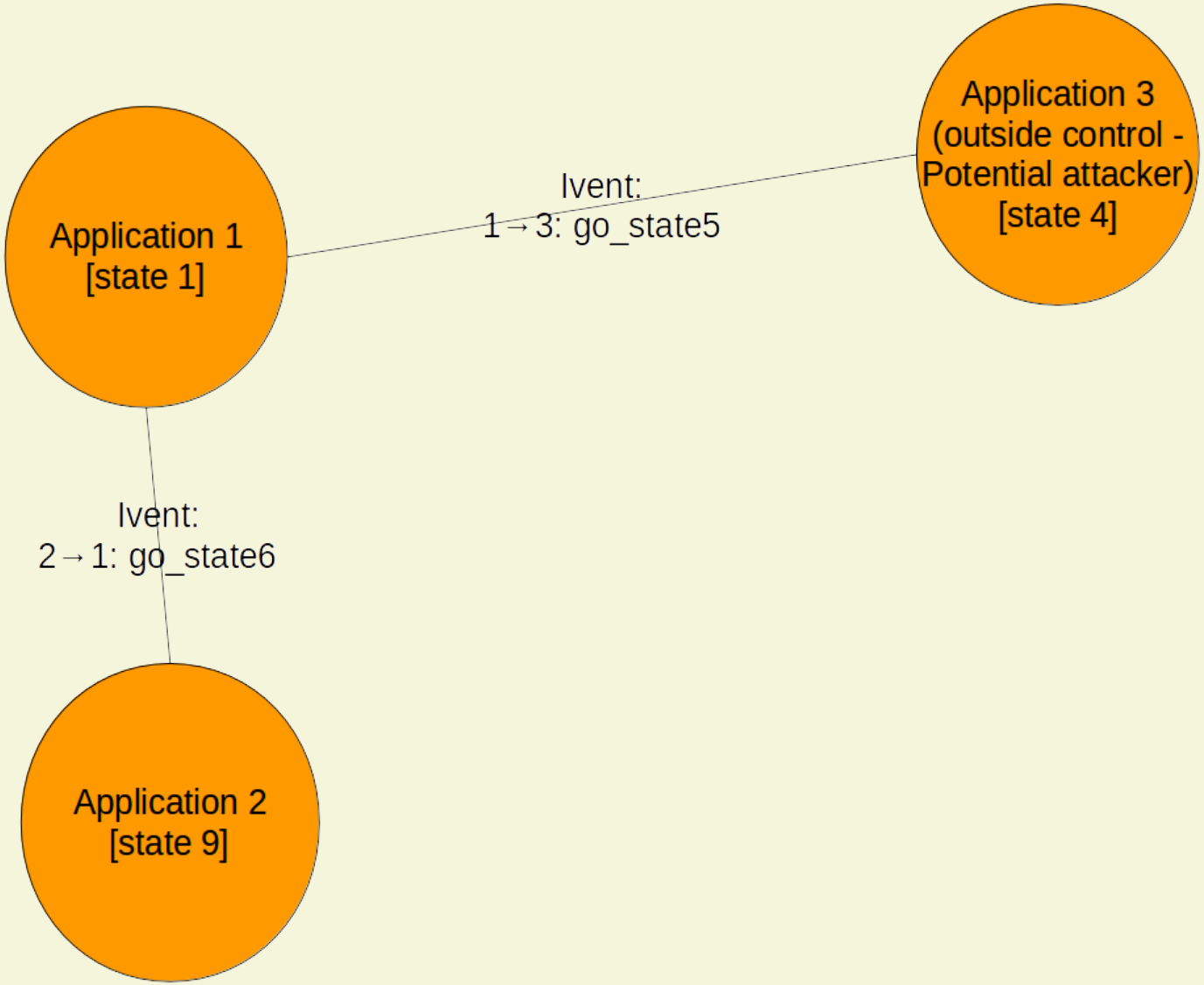
10 mars 2017

Sommaire

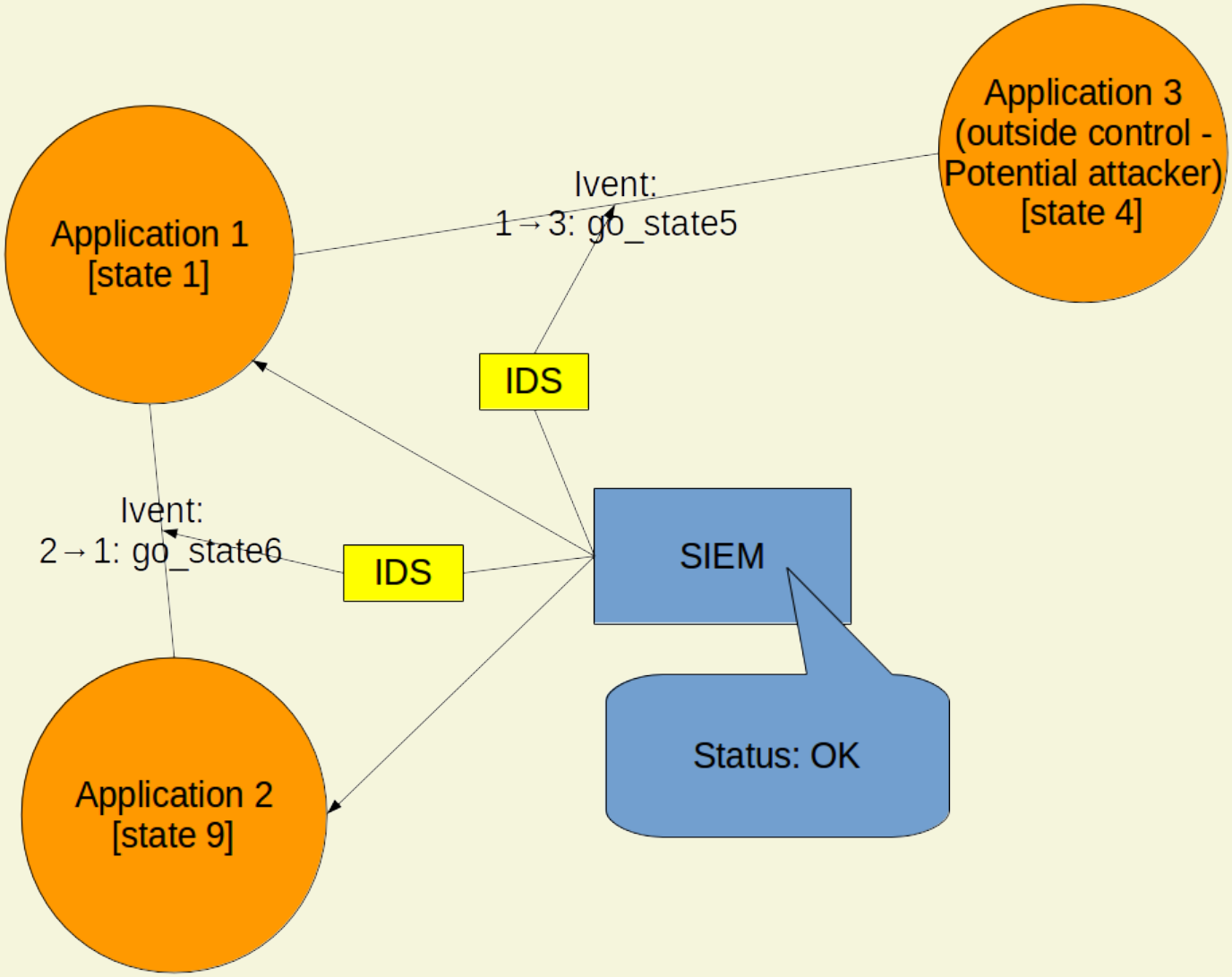
Introduction

Sommaire

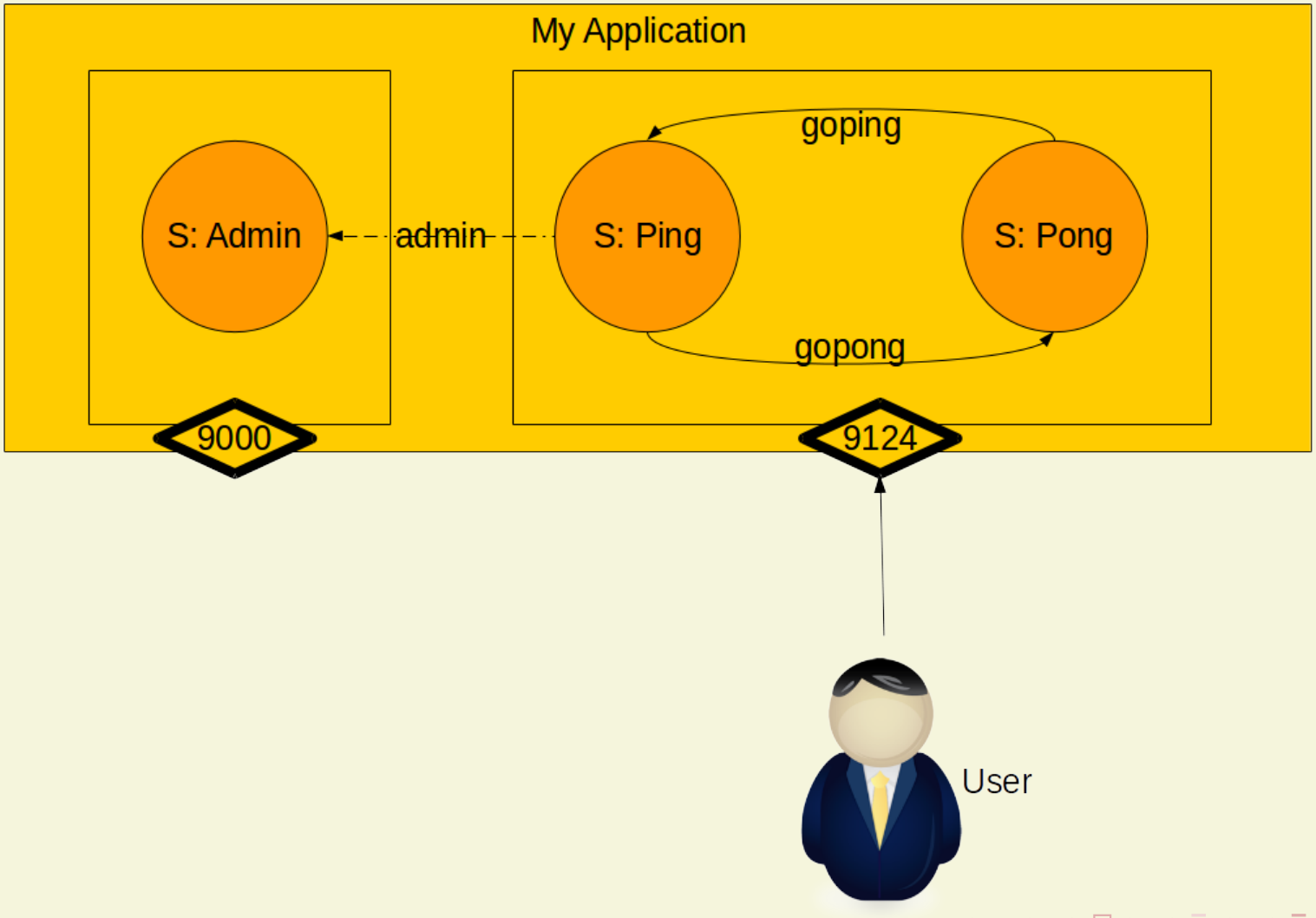
Aim of the project



Technical choices : probes



Technical choices : field of study



Organization

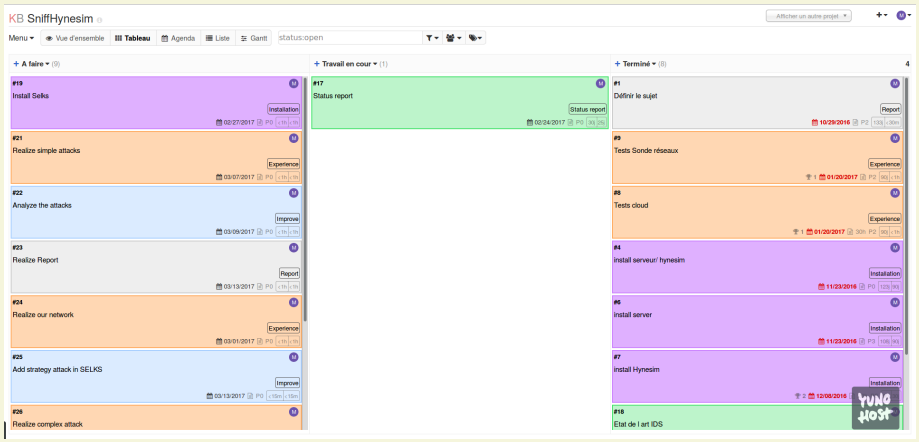


FIGURE – Kanban

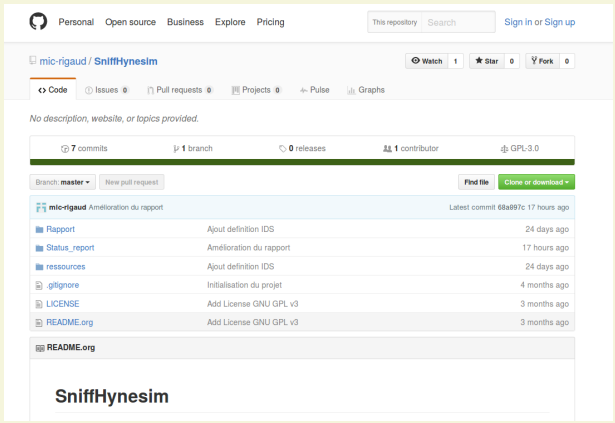


FIGURE – Github

Sommaire

Installation

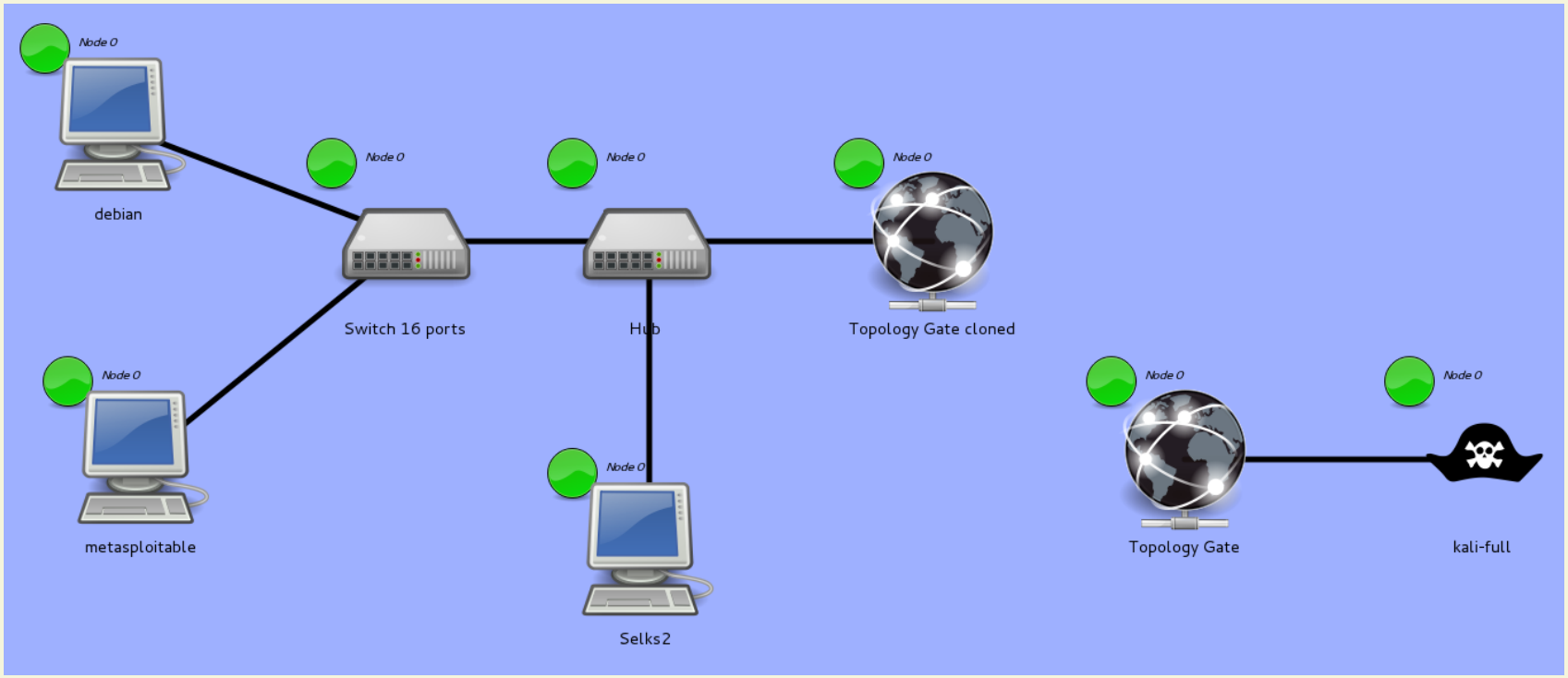


FIGURE – Network installed

Application

IDS

SIEM : Application probe

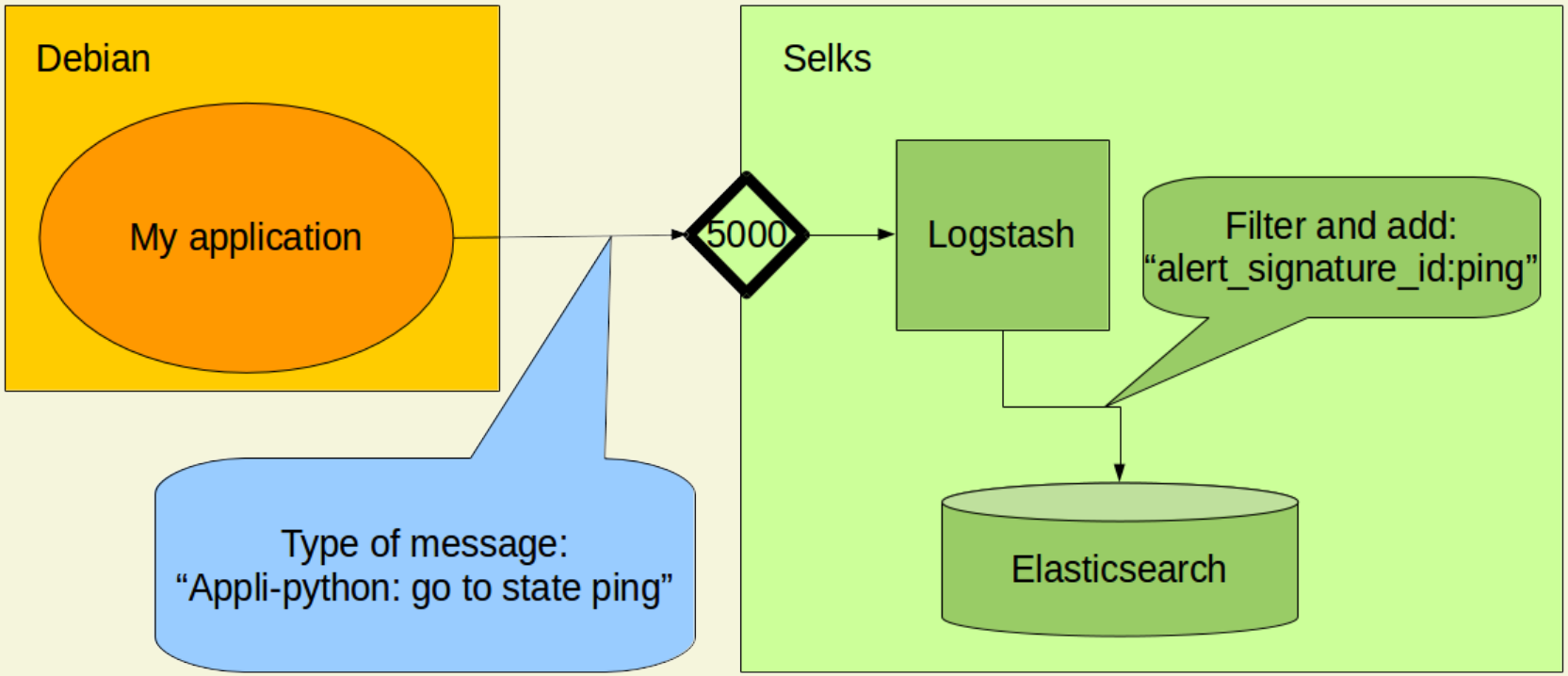


FIGURE – Data processing

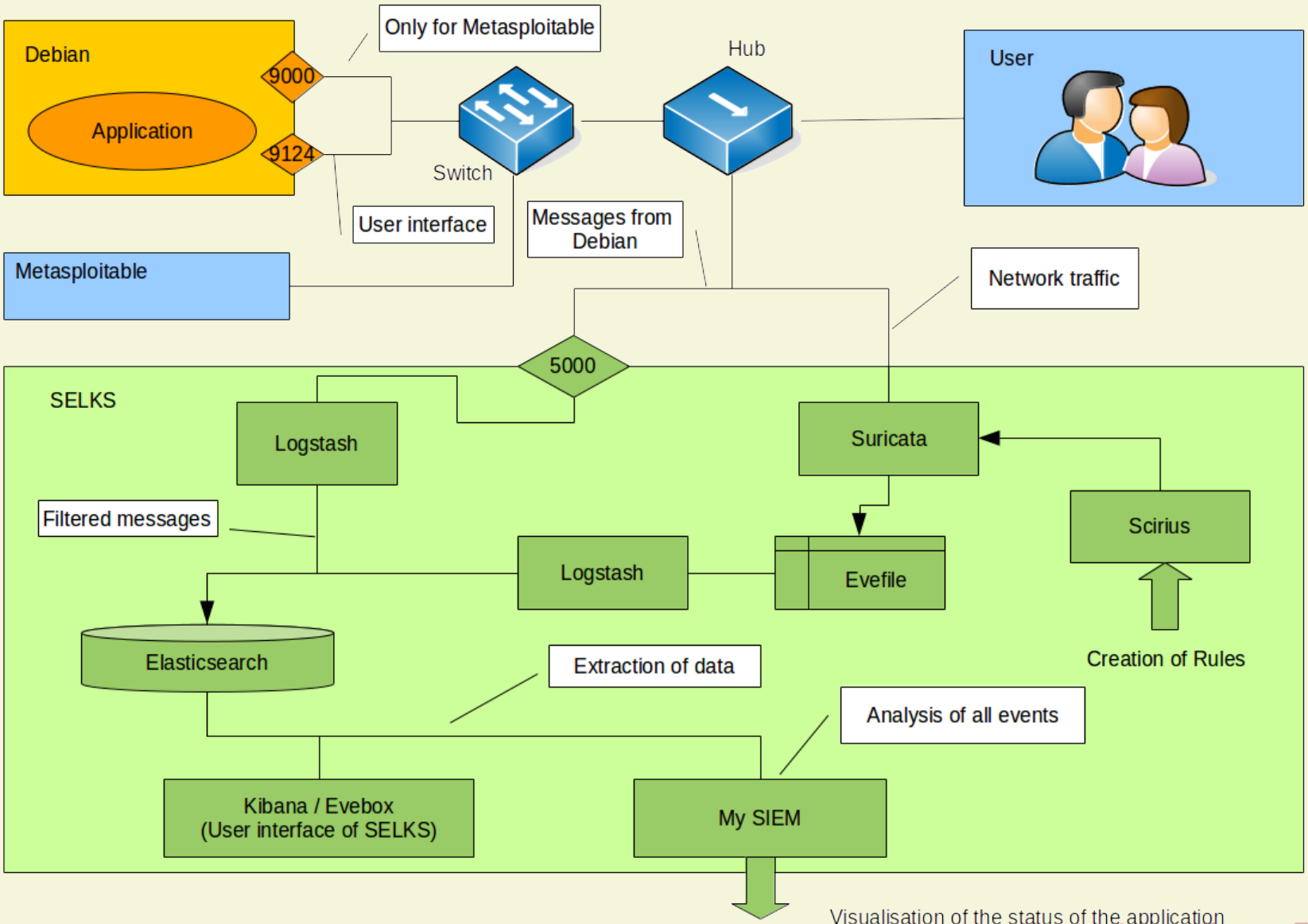
SIEM : Implementation

```
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

Sommaire

Detection system



Results

Way of improvements

Sommaire

Conclusion

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.

ENSTA Bretagne

Questions ?