ベロトス部トスミトスミナ

## Sniff Hynesim

IETA RIGAUD Michaël

ENSTA Bretagne

10 mars 2017





2/22

#### Sommaire

1 Introduction

Introduction





ベロトス部トスミトスミナ



3 / 22

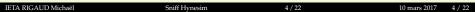
IETA RIGAUD Michaël Sniff Hynesim 3/22 10 mars 2017

イロン 不倒り 不足り 不足り

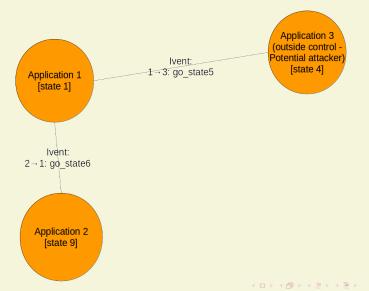
#### Sommaire

- 2 Presentation of the project Aim of the project Technical choices Organization





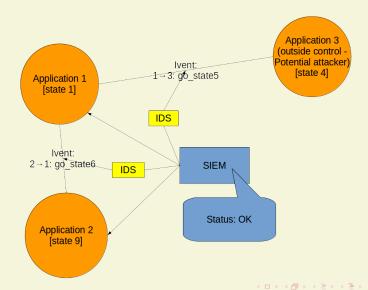
## Aim of the project





 IETA RIGAUD Michaël
 Sniff Hynesim
 5 / 22
 10 mars 2017
 5 / 22

### Technical choices: probes

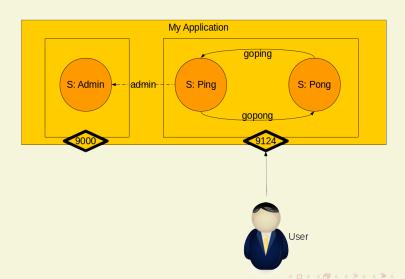




6 / 22

IETA RIGAUD Michaël Sniff Hynesim 6/22 10 mars 2017

## Technical choices: field of study





 IETA RIGAUD Michaël
 Sniff Hynesim
 7 / 22
 10 mars 2017
 7 / 22

Presentation of the project Technical contribution Results Conclusion Référence

○○○

○○○

○○○

○○○

○○○

○○○

## Organization



FIGURE – Kanban



FIGURE - Github

イロン 不倒り 不足り 不足り



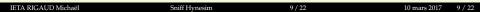
IETA RIGAUD Michaël Sniff Hynesim 8 / 22 10 mars 2017 8 / 22

《四》《圖》《意》《意》

#### Sommaire

- Introduction
- 2 Presentation of the project
- Technical contribution Installation Application IDS SIEM
- 4 Results
- 6 Conclusion





Presentation of the project **Technical contribution** Results Conclusion Références

#### Installation

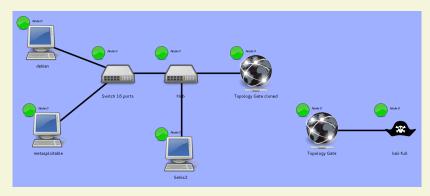


FIGURE - Network installed





ベロト (部) (意) (意)



Presentation of the project **Technical contribution** Results Conclusion Référence 0000 000 000 000

### **IDS**



ベロトス部トスミトスミト

Presentation of the project **Technical contribution** Results Conclusion Références

OOOO OOO

OOO

OOO

Technical contribution Results Conclusion Références

# SIEM : Application probe

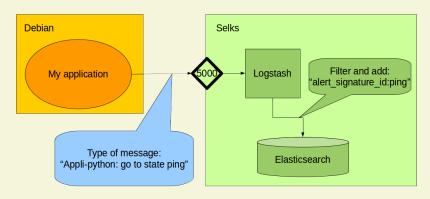


FIGURE - Data processing



IETA RIGAUD Michaël Sniff Hynesim 13 / 22 10 mars 2017 13 / 22

### SIEM: Implementation

Introduction

FIGURE - My SIEM



イロト (例) (注) (注)

IETA RIGAUD Michaël Sniff Hynesim 14/2 10 mars 2017 14/22

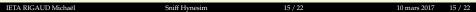
《四》《圖》《意》《意》

### Sommaire

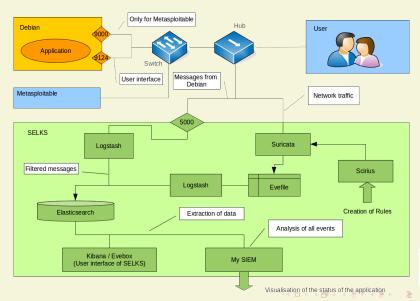
- A Results

Detection system Results Way of improvements





### Detection system





16 / 22

IETA RIGAUD Michaël Sniff Hynesim 16 / 22 10 mars 2017

ベロト (部) (意) (意)

### Results



ベロトス部トスミナスミト

# Way of improvements



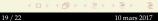
IETA RIGAUD Michaël Sniff Hynesim 18 / 22 10 mars 2017 18 / 22

#### Sommaire

- **6** Conclusion



19 / 22



ベロト (部) (意) (意)



20 / 22

イロン 不倒り 不足り 不足り

# 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.



IETA RIGAUD Michaël Sniff Hynesim 21 / 22 10 mars 2017 21 / 22

ベロトス部トスミナスミト

### Questions?





IETA RIGAUD Michaël Sniff Hynesim 22 / 22 10 mars 2017 22 / 22