



PROJET S.O.C.

 🔍 🎙



LE SOMMAIRE

01

Introduction

02

Schéma du SOC

03

Gestion de projet

04

Justificatif des
choix
technologiques

05

Plan de
sensibilisation

06

Résultats attendus

07

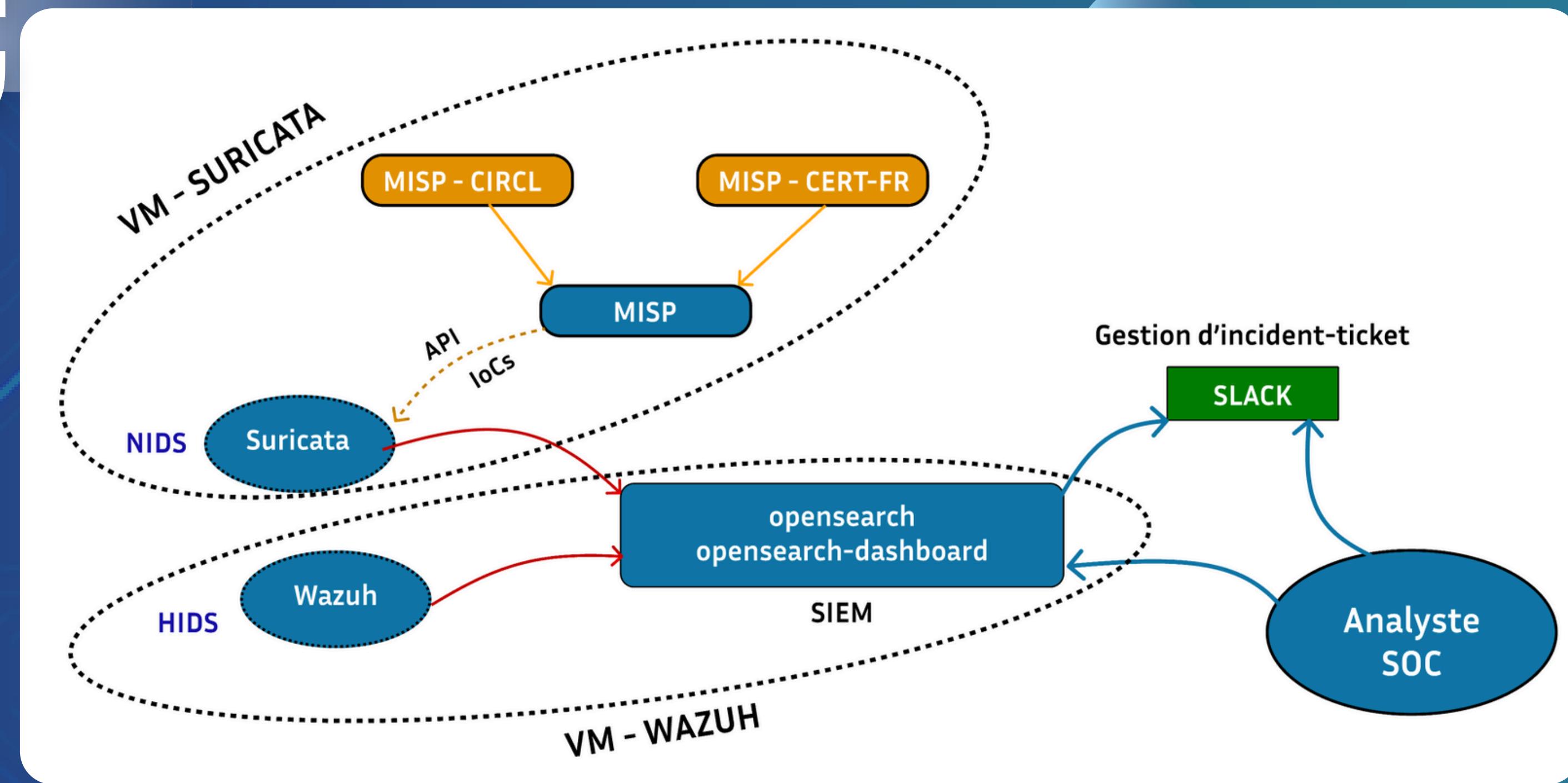
Conclusion /
Démo



INTRODUCTION

SCHÉMA SOC

04/10

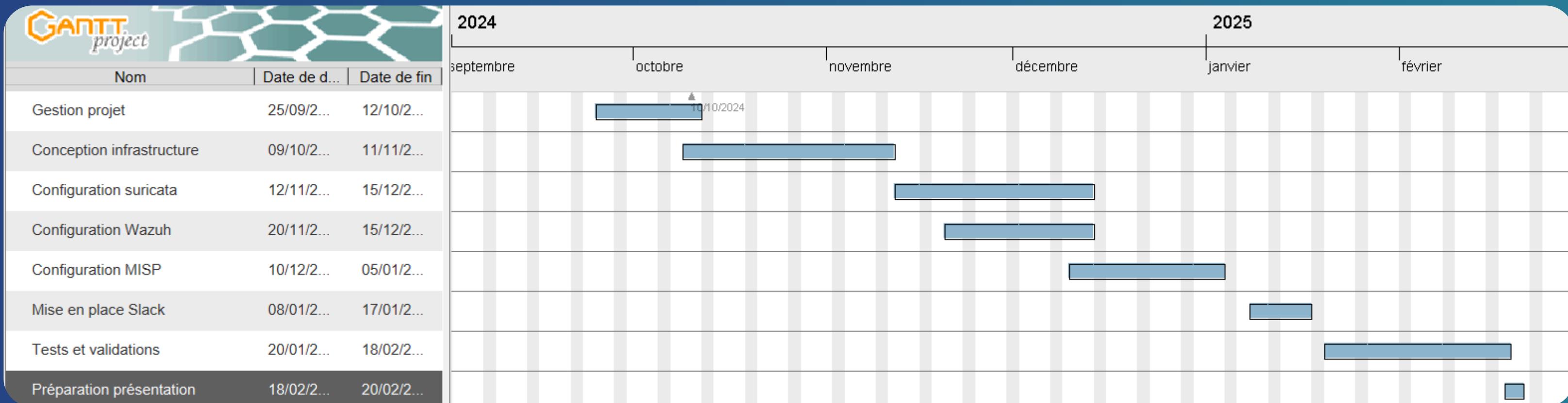




GESTION DE PROJET

05/10

LE GANTT





MÉTHODE R.A.C.I

- R : Responsable
- A : Approbateur
- C : Consulté
- I : Informé

UVRABLES/ACTIVITÉS LIÉS AU PROJET	Aziz	Emmanuel	Alexandre	Ricardo	Mohcine	Mr BALDE
1. Gestion de projet	R	A C	A C	A C	A C	I
2. Conception de l'infrastructure	C	R	C	C	C	C A
3. Configuration Suricata	A C	A C	C	R	C	I
4. Configuration Wazuh	C	R	C	C	R	I
5. Configuration du MISP	R	C	C	C	C	I
6. Mise en place du Slack	C	C	R	C	R	I
7. Tests et validation	A R	A R	A R	A R	A R	A
8. Présentation	R	R	R	R	R	A



CHOIX TECHNIQUE

MISP

- collecter
- stocker
- analyser
- partager

open source

1

Suricata

- Détection réseau
- Performance
- Flexible

2

Wazuh:

3

- Détection machine
- Analyse
- Dashboard

Slack:

4

- Communication
- Facile à mettre en place

PLAN DE SENSIBILISATION



08/10

INTÉGRATION DE THREAT INTELLIGENCE

Le SOC peut identifier des domaines, des adresses IP ou des pièces jointes malveillantes associées à des campagnes de phishing connues

UTILISATION DE SIEM

Un SIEM (Security Information and Event Management) permet de corrélérer les événements liés à des campagnes de phishing

MISE EN PLACE DE SOLUTIONS

Secure Email Gateway (SEG) pour filtrer les emails malveillants avant qu'ils n'atteignent les utilisateurs.

MISE À JOUR DES SYSTÈMES

En surveillant les vulnérabilités à jour (patch management), le SOC peut prévenir les attaques de type phishing exploitant des failles

BLOCAGE AVEC DES RÈGLES IDS/IPS

Des solutions comme Suricata, configurées avec des IOCs peuvent bloquer des communications avec des sites de phishing.



RÉSULTATS ATTENDUS

- BANNISSEMENT DES ADRESSES IP RÉPERTORIÉES PAR DES ORGANISMES FIABLES (MISP.RULES)
- ALERTES SLACK SUR CHAQUE TENTATIVE DE CONNEXION PAR UNE ADRESSE BLACKLISTÉE
- RETOUR EN TEMPS RÉEL DES PERFORMANCES DES SERVICES SUR LE DASHBOARD WAZUH
- SUIVI DES ALERTES RÉSEAU VIA LE DASHBOARD WAZUH

CONCLUSION