# Projet d'étude Cybersécurité

Mise en place d'un SOC (***Security Operation Center*** )

BUT3-DACS 2024-2025

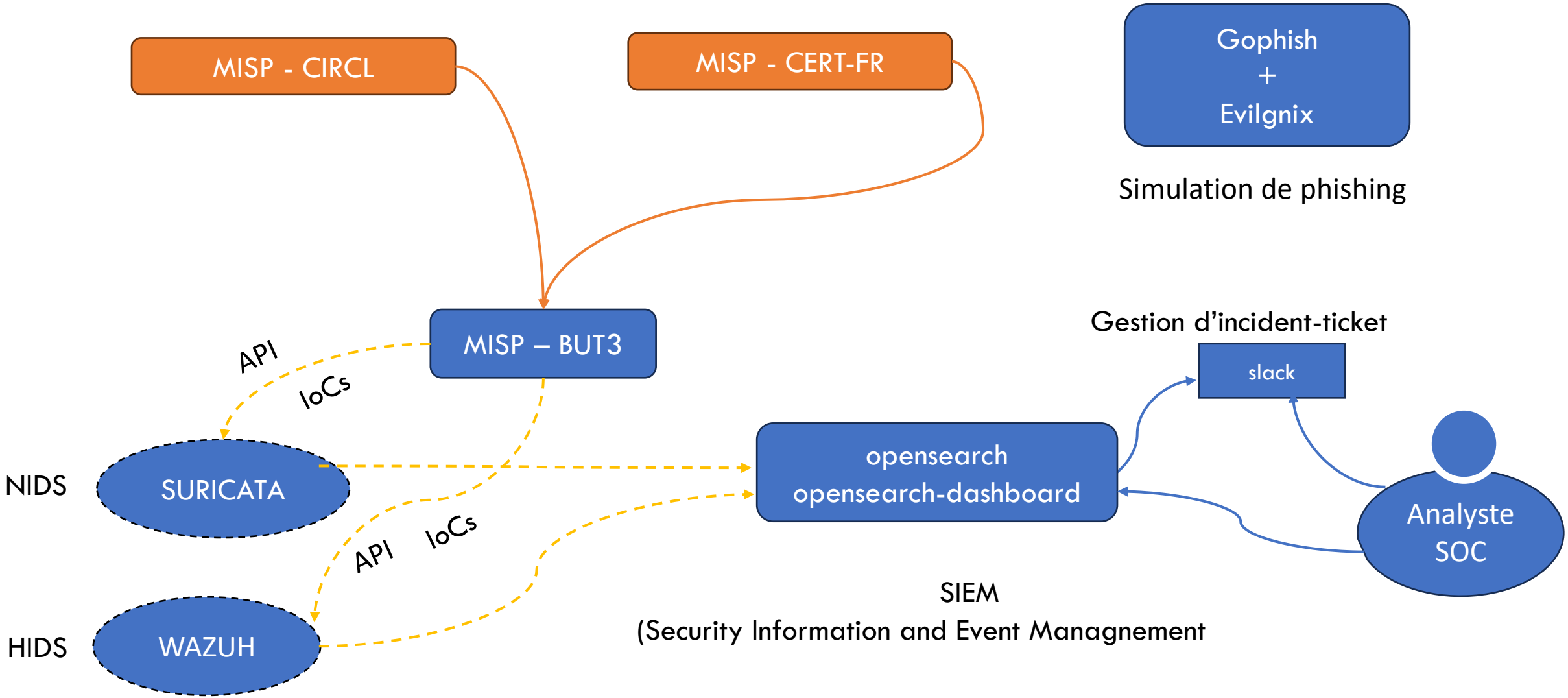
# Organisation de votre SOC

Votre SOC a pour objectif de répondre aux exigences de sécurité informatique de toutes les activités de votre entreprise.

Elle est basé sur 5 concepts clés :

1. **Partager** l'information avec les différents acteurs partenaires de notre entreprise.
2. **Surveiller** l'activité réseau de votre entreprise pour répondre aux plus vite aux atteintes à la sécurité de notre entreprise.
3. **Consolider** l'information afin d'avoir une vision globale de la sécurité de votre entreprise.
4. **Alerter** les différents acteurs (administrateurs systèmes, Ingénieur réseau et sécurité) des activités anormales détectées.
5. **Sensibiliser** les différents acteurs aux enjeux de sécurité informatique.

# Le workflow à implémenter



# Consignes pour ce projet :

1. Pour ce projet vous aurez besoin de 4 machines (misp, attaquant, serveur et siem).
2. Les 4 machines peuvent être soit au format vm ou docker.
3. Le choix du OS est entre Ubuntu ou Redhat
4. Toutes les machines seront sur un même sous-réseau.
5. Libre à vous de choisir votre scenario d'attaque, de détection et de réponse à l'incident.

# Travail attendu à la fin du projet:

1. Présentation du travail de votre équipe sous format power point :
    1. Schéma de votre SOC (Security Operation Center)
    2. Méthode de gestion du projet utilisé
    3. Justificatif des choix technologiques
    4. Présenter votre plan de sensibilisation au phishing
    5. Résultats obtenus et bilans

2. Recette du projet :
    1. Présentation de l'architecture technique
    2. Démonstration de votre maquette
    3. Votre plan de réponse à l'incident