

Implémentation d'un SIEM

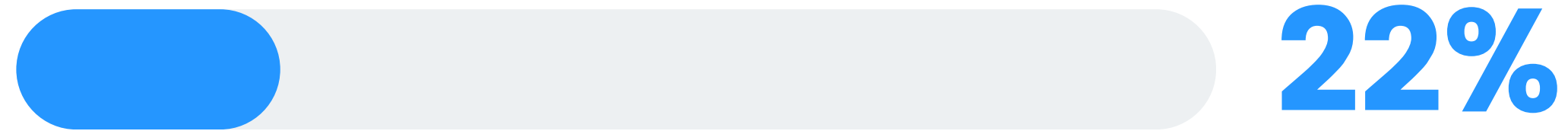
Pour la supervision de la sécurité au niveau
du réseau de l'ESI

- Equipe 3 -



SDG 8: Decent Work and Economic Growth

In 2019



of the world's youth were not engaged in either education, employment, or training.

There is a continued lack of decent work opportunities, insufficient investments, and under-consumption.

Plan de la présentation



01

Qui sommes-nous?

02

Partie 1 : SIEM

03

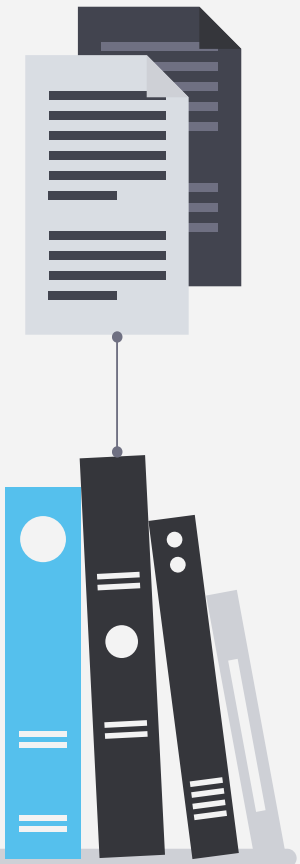
Partie 2 : Étude comparative

04

Solution proposée

05

Conclusion

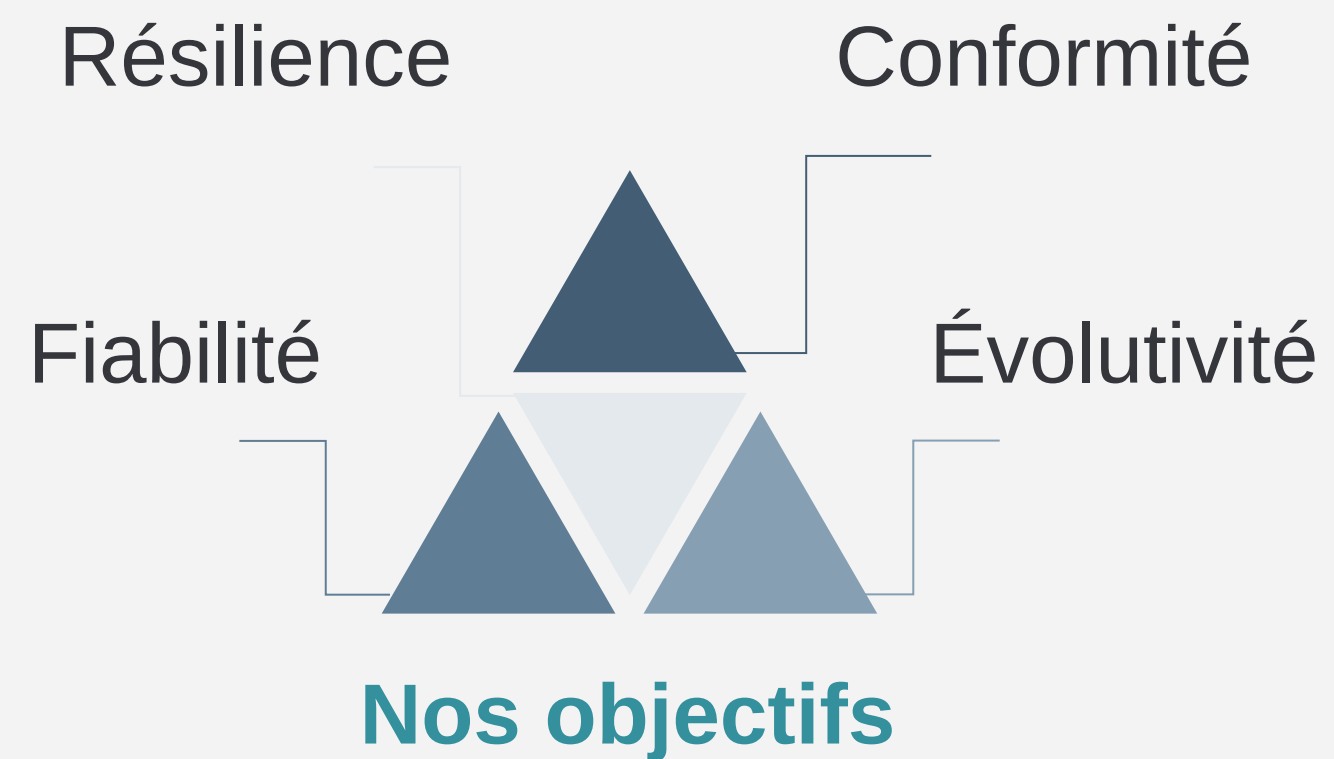




01 Qui sommes-nous?

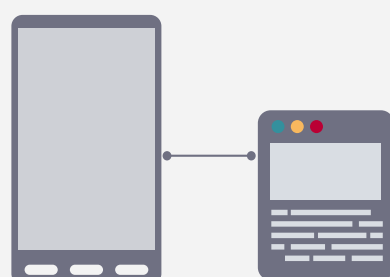
Présentation de notre expertise et notre équipe projet.

Entreprise

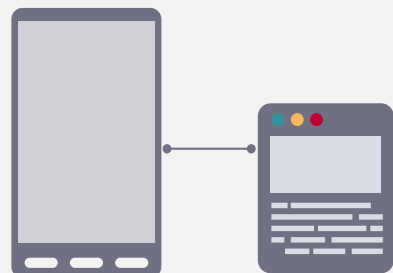
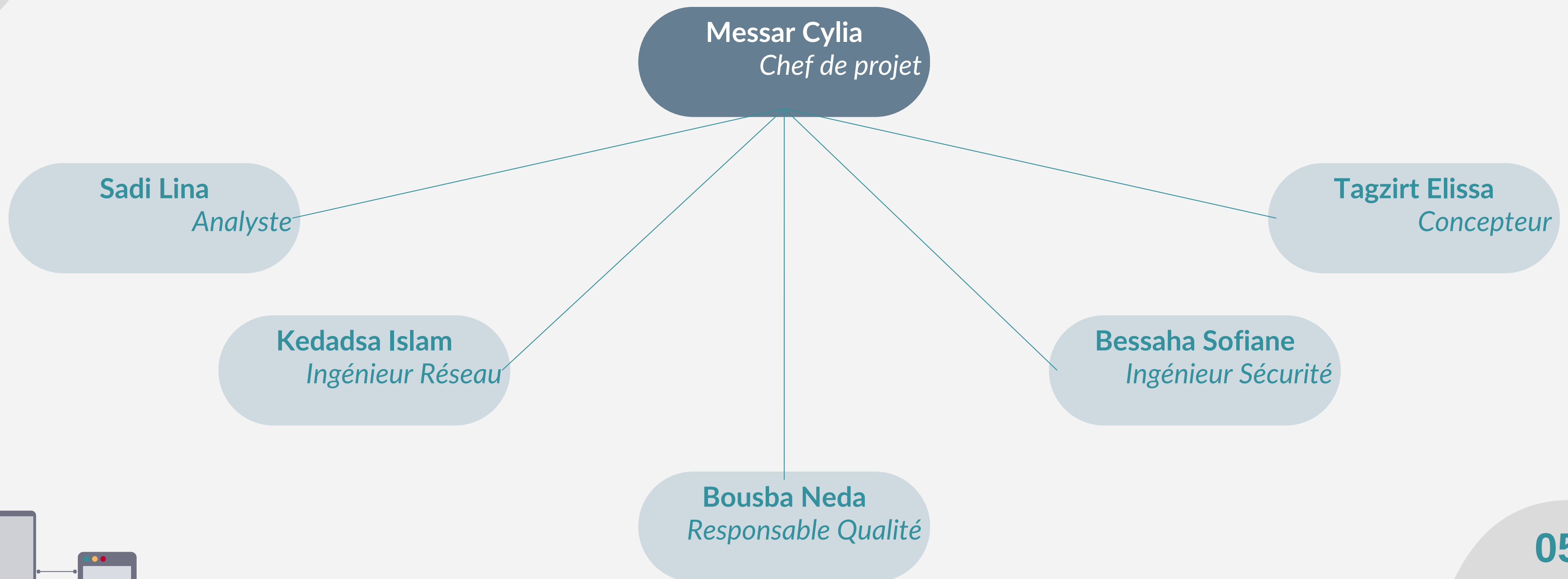


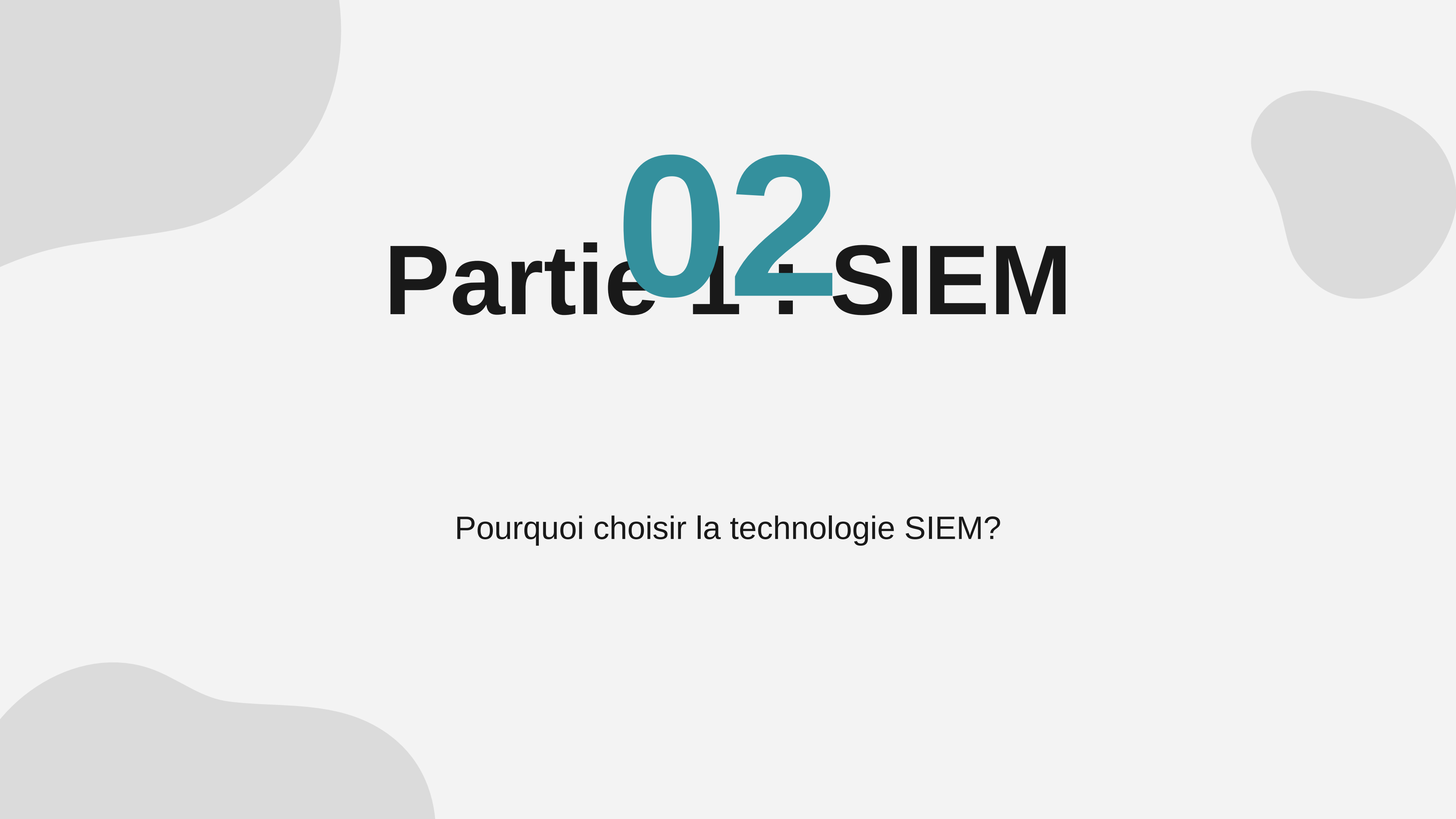
SMART NET

SAFE, MANAGED, ACCESSIBLE, RELIABLE, AND TRUSTED NETWORK



Équipe projet





02 Partie 1 : SIEM

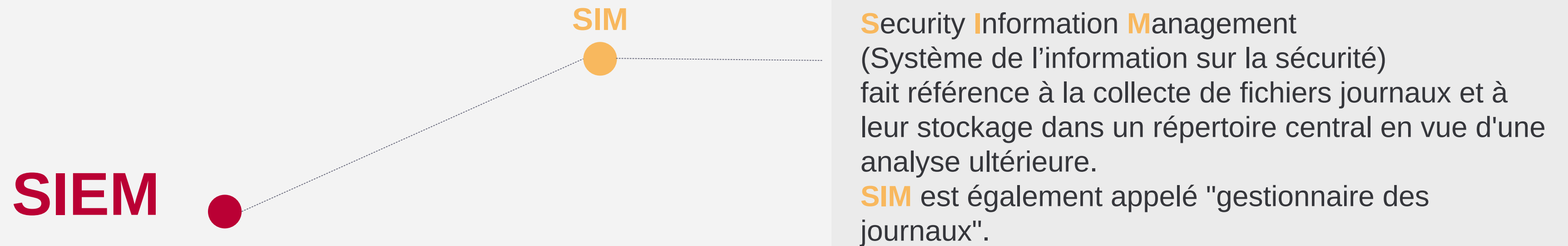
Pourquoi choisir la technologie SIEM?

2- Définition du SIEM



Security **I**nformation **M**anagement
(Système de l'information sur la sécurité)
fait référence à la collecte de fichiers journaux et à
leur stockage dans un répertoire central en vue d'une
analyse ultérieure.
SIM est également appelé "gestionnaire des
journaux".

2- Définition du SIEM



2- Définition de SIEM



SIEM



SEM



Security Event Management

(La gestion des événements de sécurité) est l'identification, la collecte, la surveillance, l'évaluation, la corrélation et le contrôle des événements et des alertes du système.

D'une certaine manière, le **SEM** est une amélioration de SIM, même si les deux sont considérés comme des domaines distincts de la gestion de la sécurité.

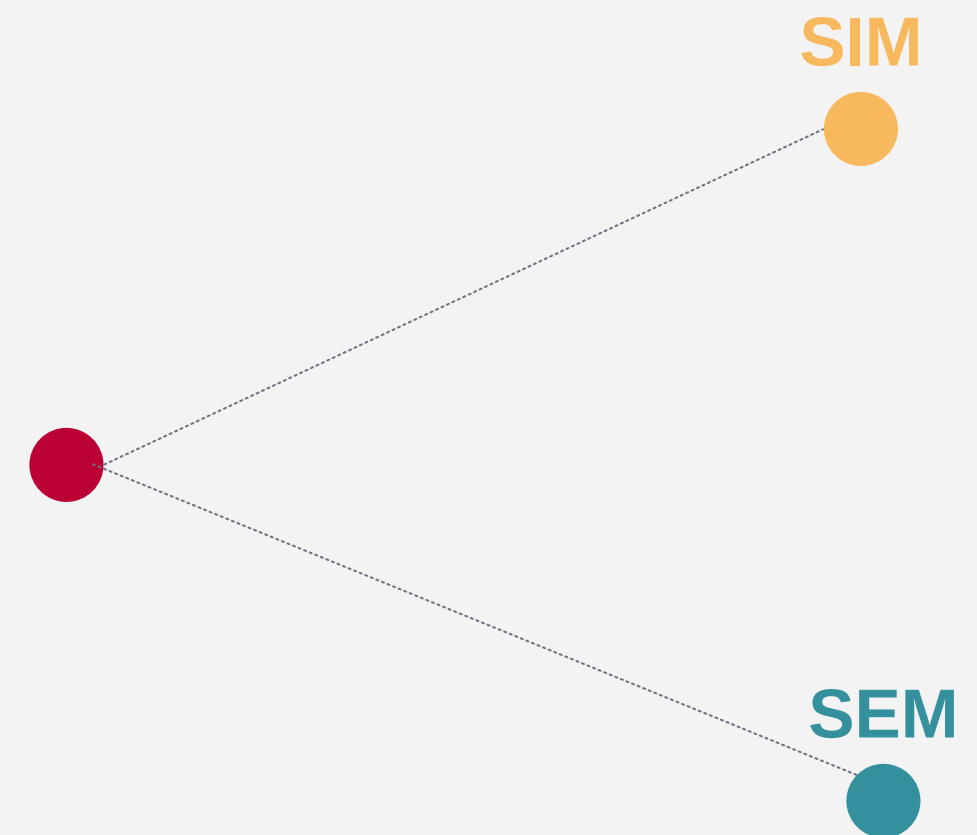
2- Définition de SIEM



Les SIEM(Security Information and Event Management) constituent la plate-forme centrale des centres d'opérations de **sécurité modernes**.

Le SIEM est un outil qui **collecte**, **agrège**, **normalise** les données et les **analyse** selon des règles prédéfinies et les **présente** dans un format lisible par l'homme.

SIEM



3- Fonctionnalités principales des SIEM

Collecte



IDS/IPS



Firewall



Server



Router



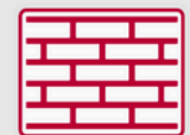
Switch

3- Fonctionnalités principales des SIEM

Collecte



IDS/IPS



Firewall



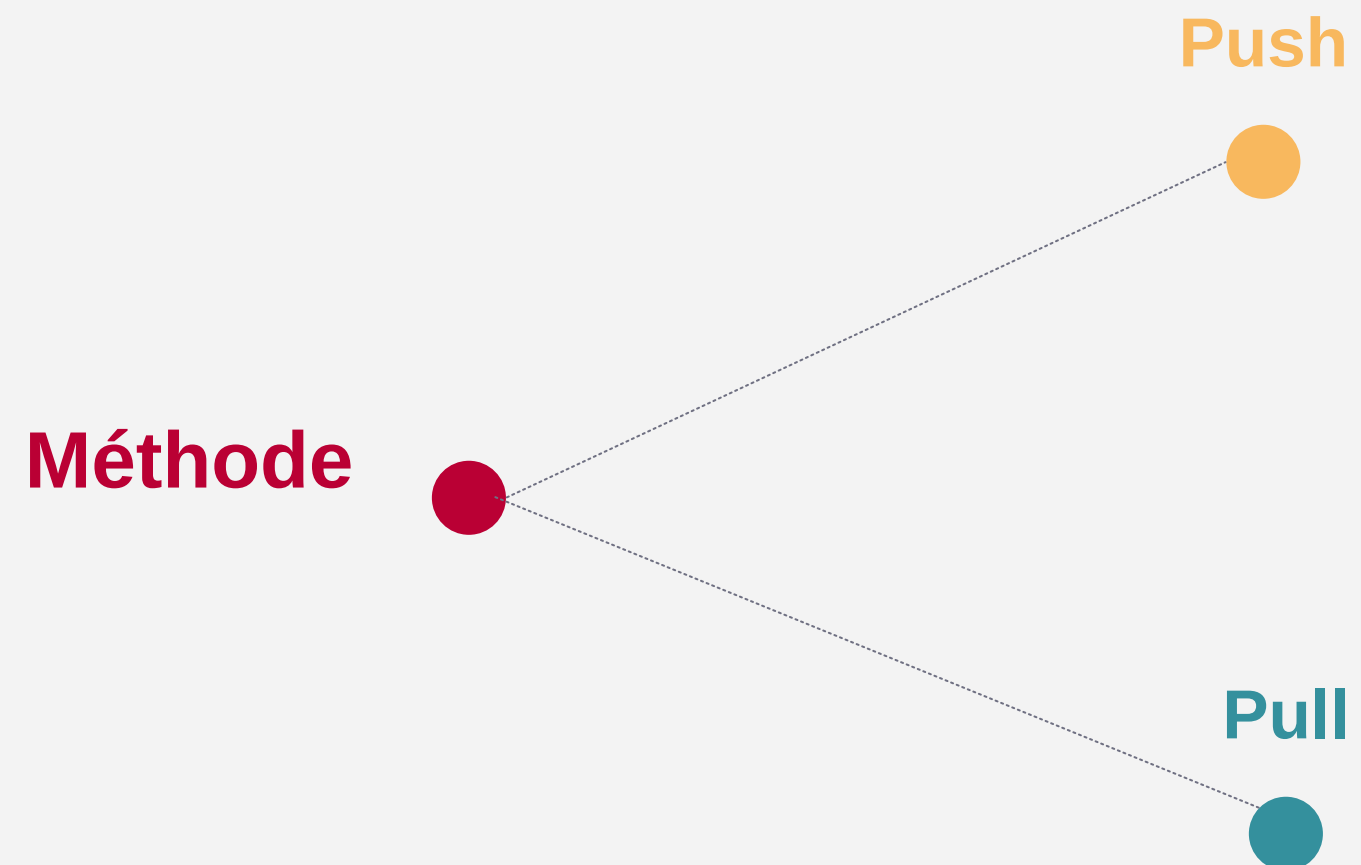
Server



Router



Switch



3- Fonctionnalités principales des SIEM

Collecte



IDS/IPS



Firewall



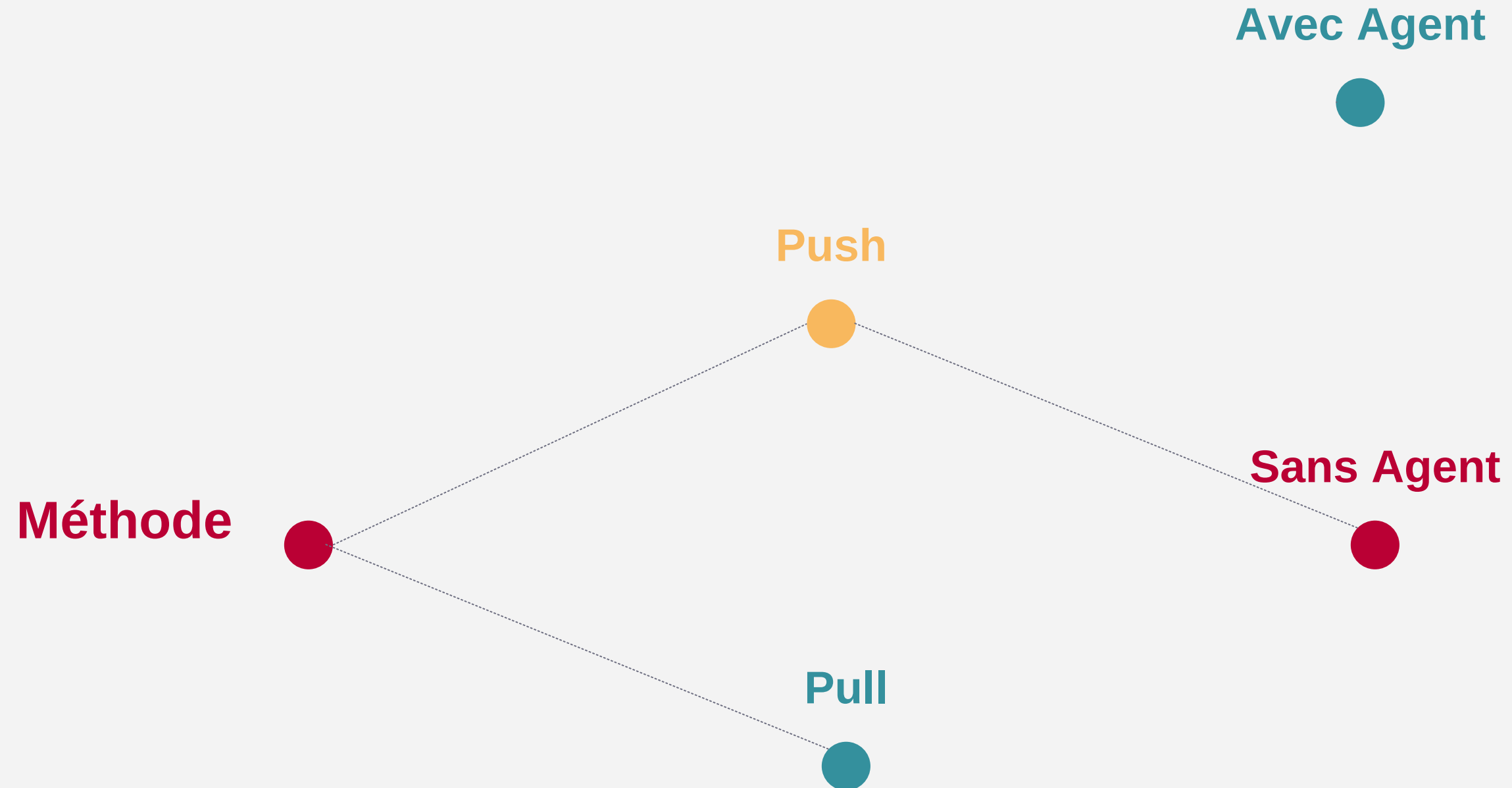
Server



Router



Switch



3- Fonctionnalités principales des SIEM

Collecte



IDS/IPS



Firewall



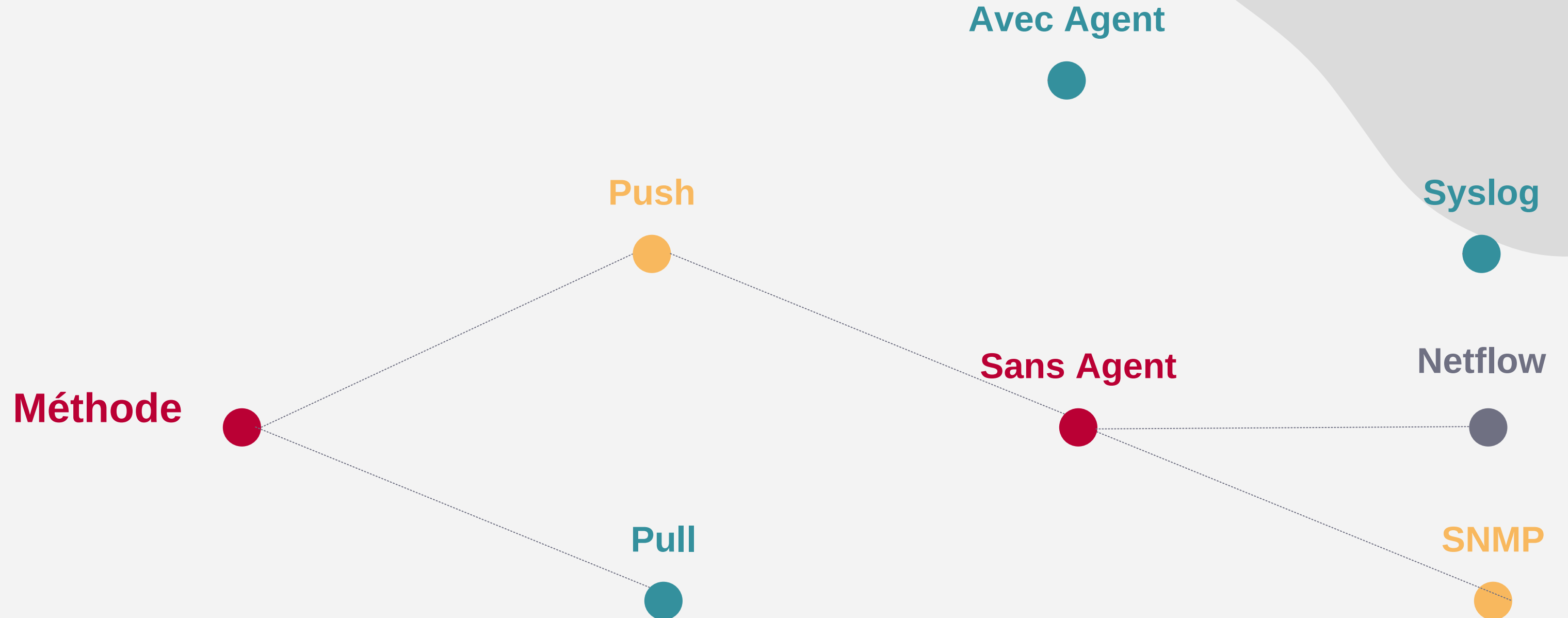
Server



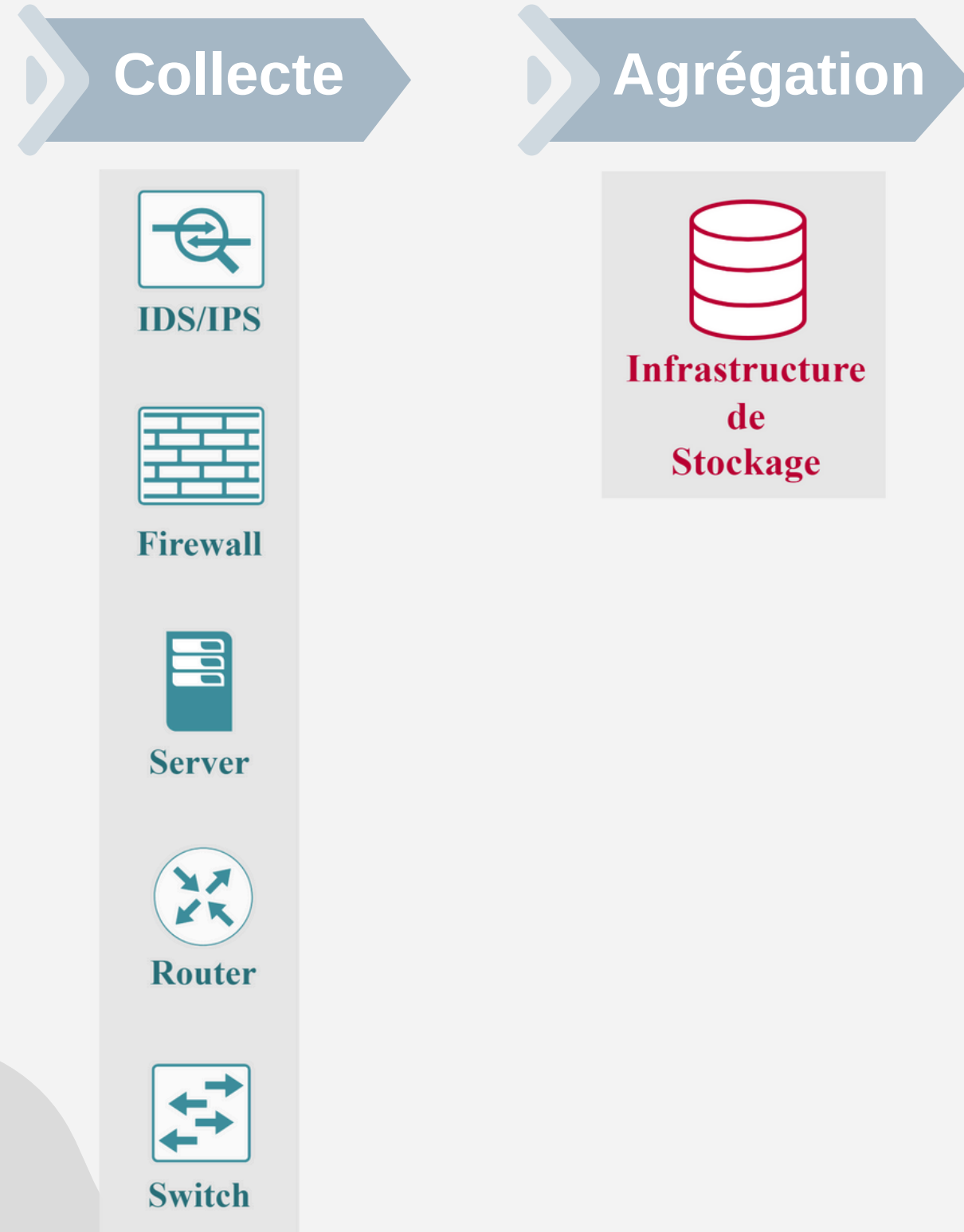
Router



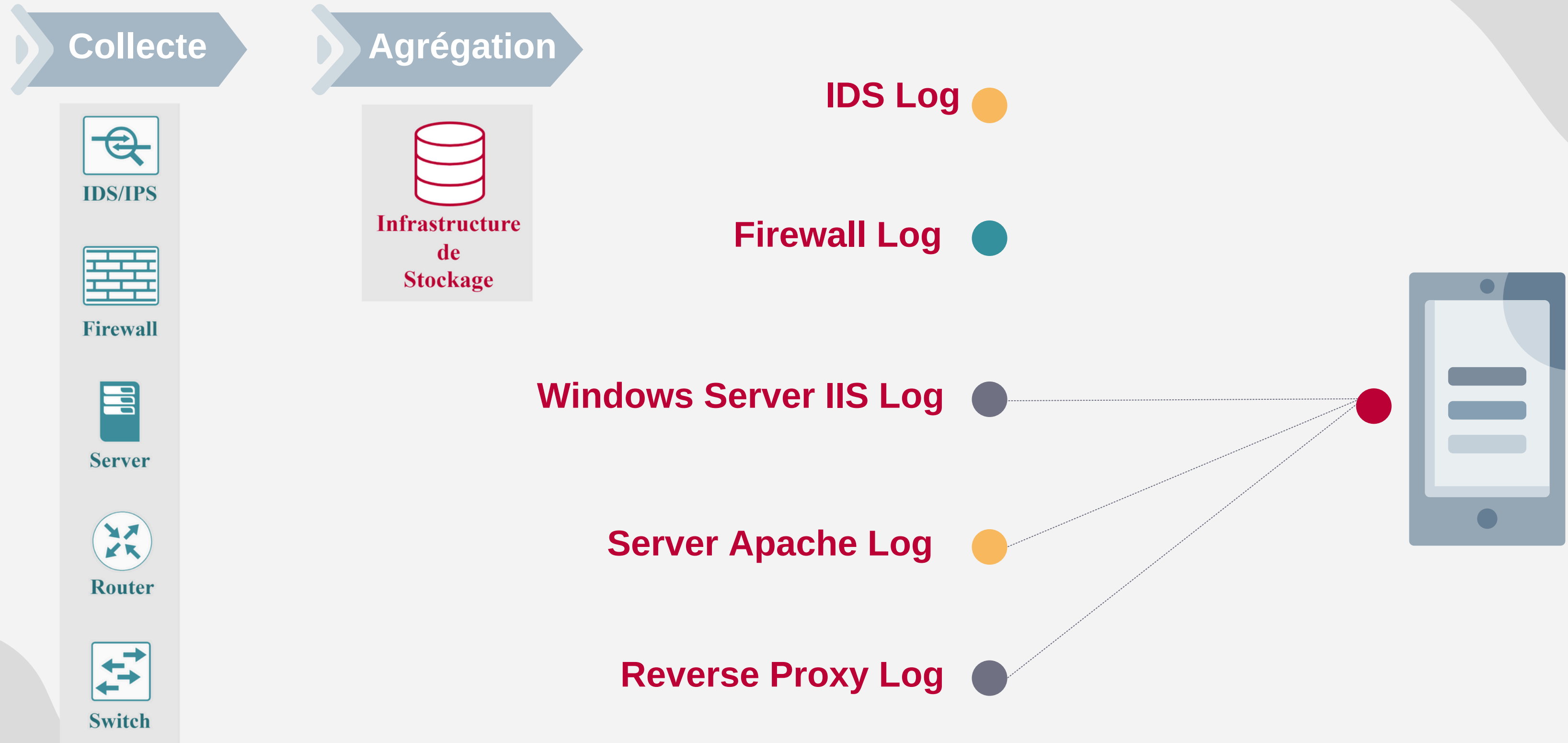
Switch



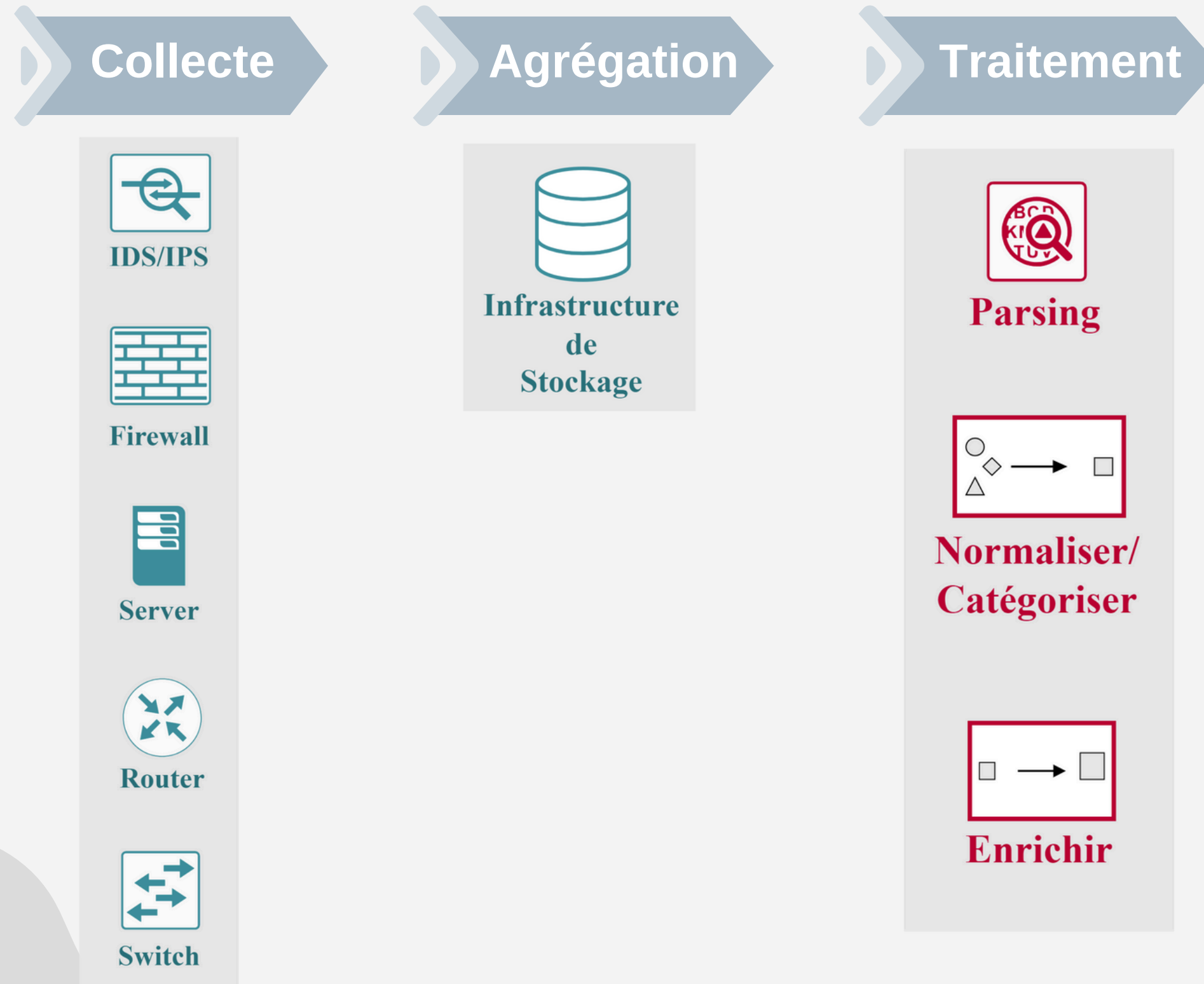
3- Fonctionnalités principales des SIEM



3- Fonctionnalités principales des SIEM



3- Fonctionnalités principales des SIEM



3- Fonctionnalités principales des SIEM

Collecte



IDS/IPS



Firewall



Server



Router



Switch

Agrégation

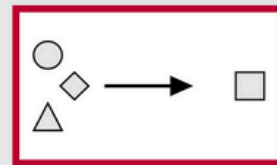


Infrastructure
de
Stockage

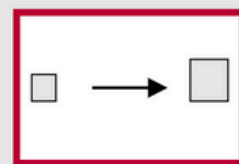
Traitement



Parsing



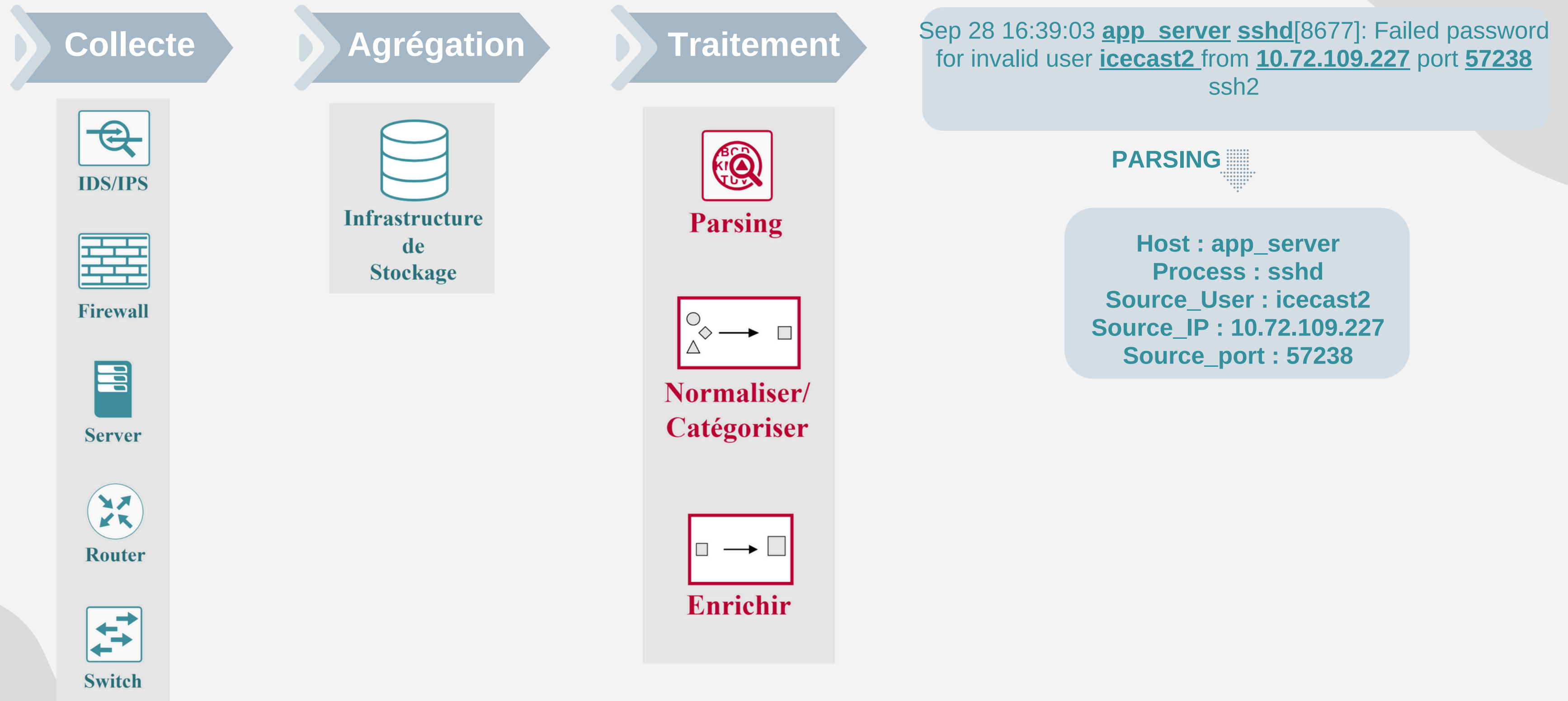
Normaliser/
Catégoriser



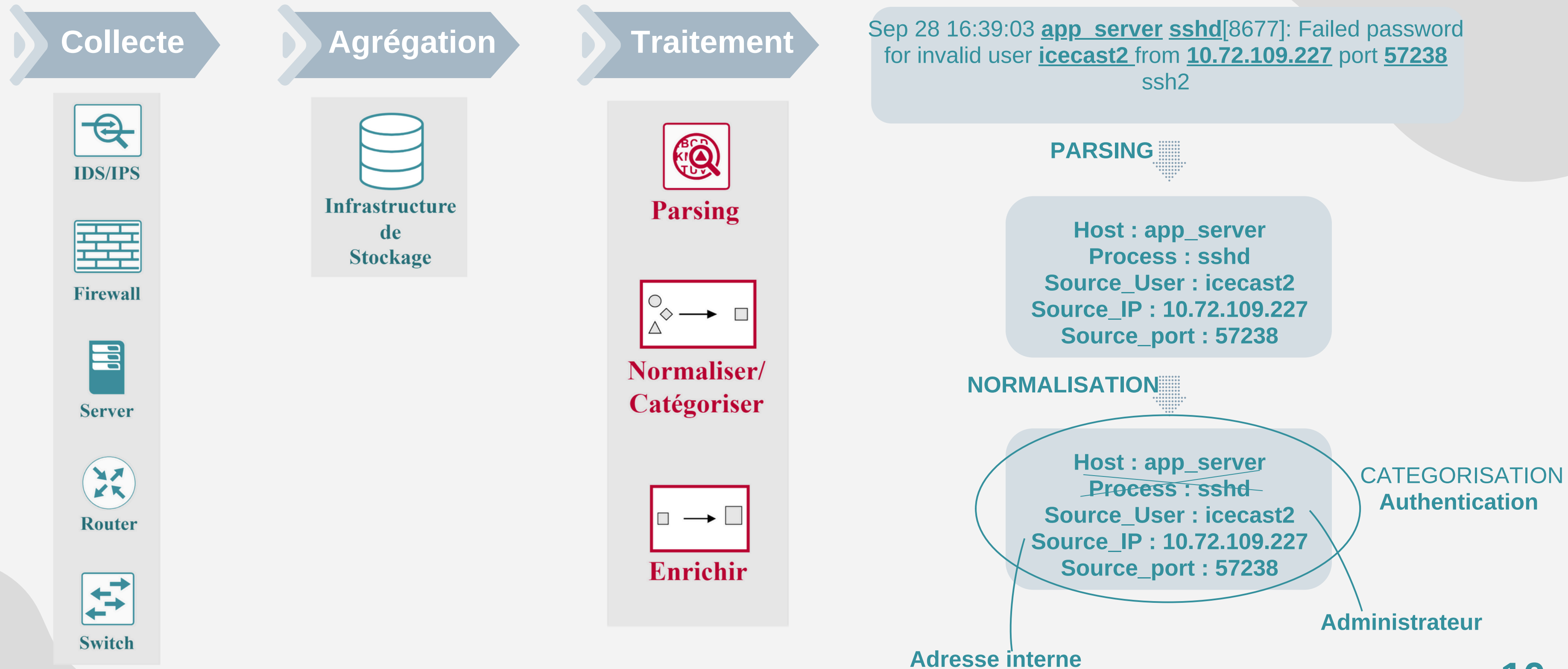
Enrichir

Sep 28 16:39:03 app_server sshd[8677]: Failed password
for invalid user icecast2 from 10.72.109.227 port 57238
ssh2

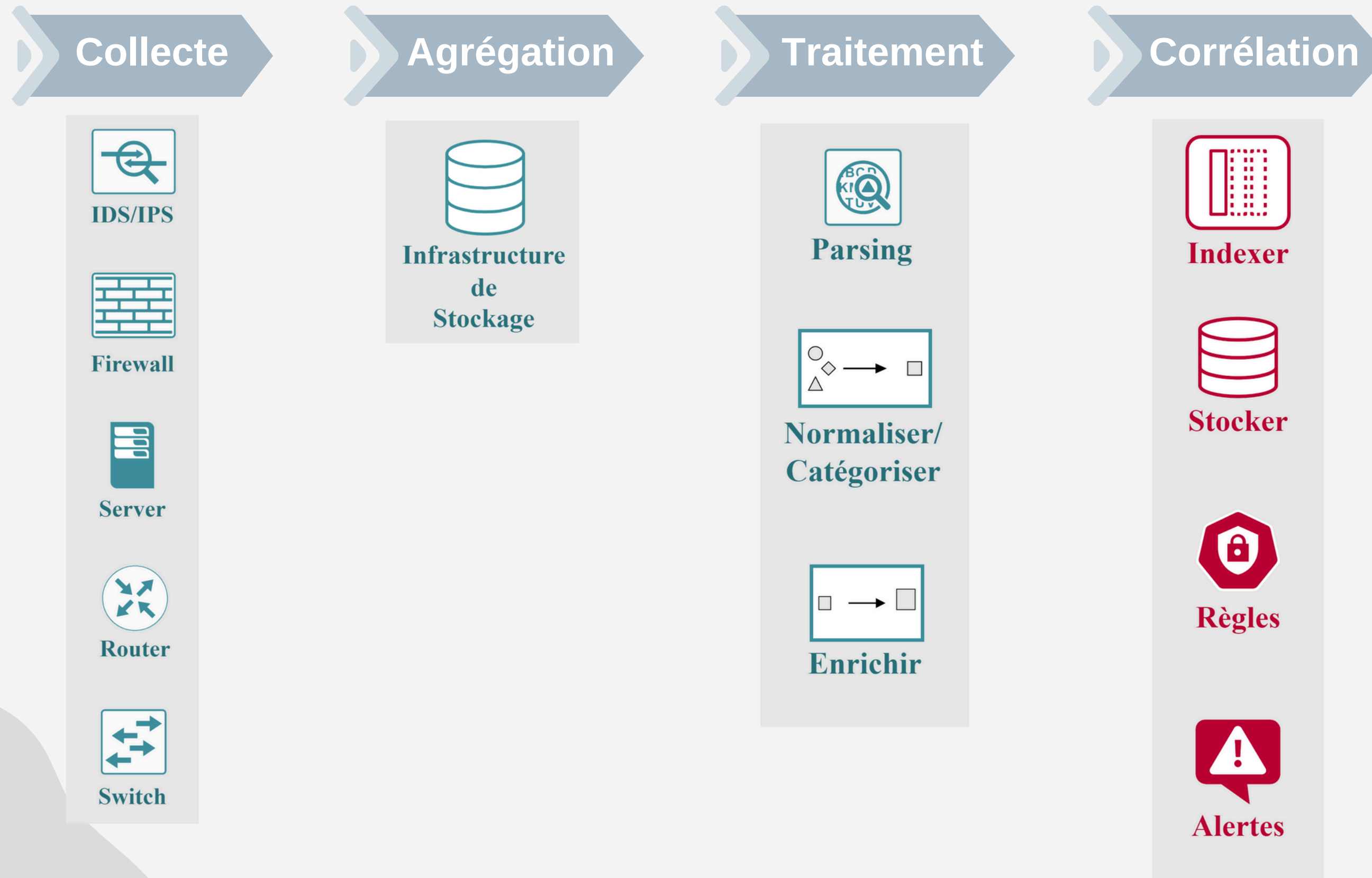
3- Fonctionnalités principales des SIEM



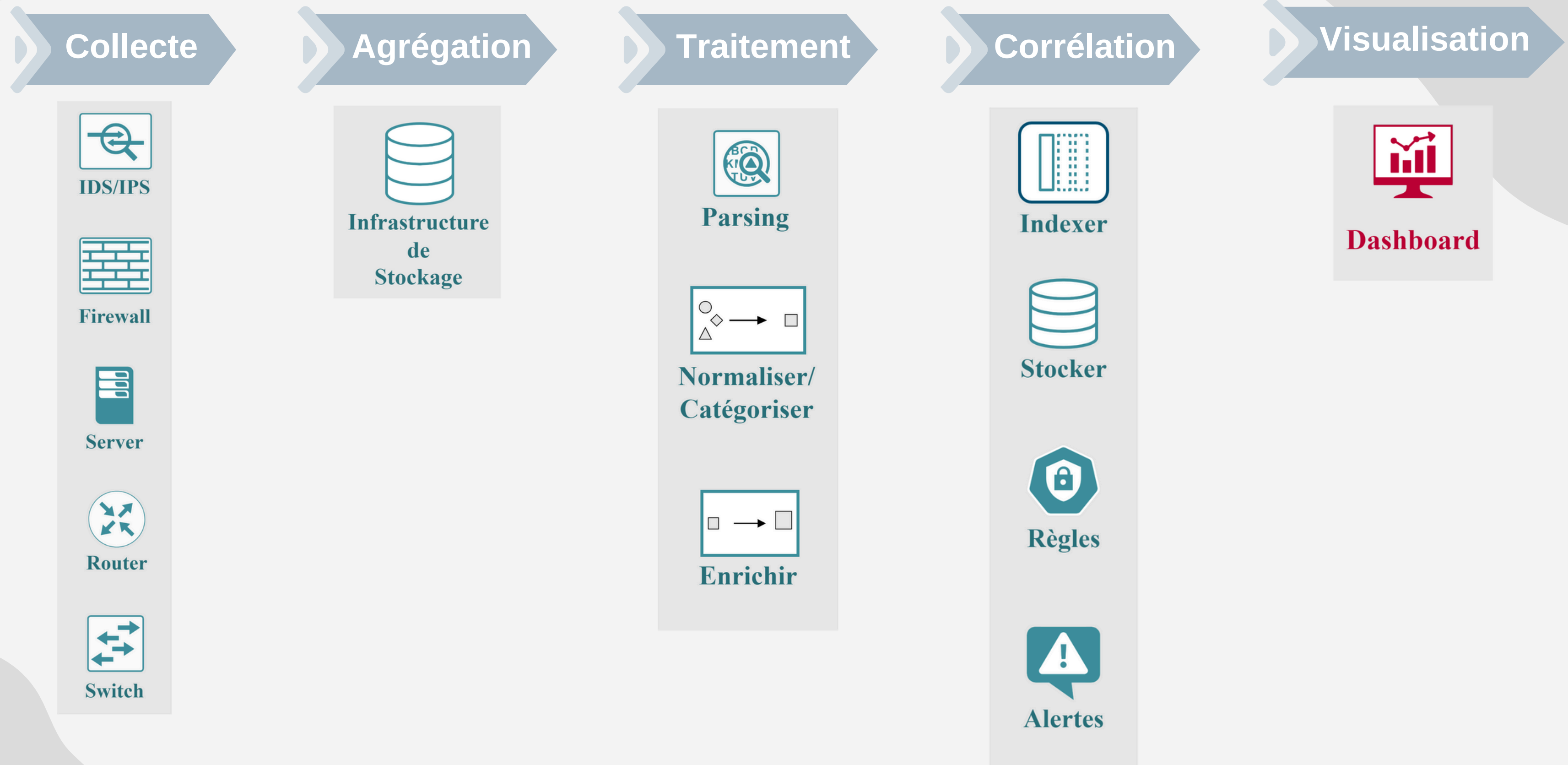
3- Fonctionnalités principales des SIEM



3- Fonctionnalités principales des SIEM



3- Fonctionnalités principales des SIEM



4- Avantages des SIEM



Intégration avec d'autres outils de sécurité.



Détection accélérée des menaces.



Gestion des Volumes Importants de Données des diverses sources.



Amélioration de la visibilité et de la conformité.



5- Inconvénients des SIEM



- ❯ Coûts et Complexité élevés.
- ❯ Maintenance et mises à jour constantes.
- ❯ Questions de confidentialité.
- ❯ Génération des faux positifs.

6- Limites des technologies SIEM



La détection des menaces inconnues ou avancées.



Surcharge d'informations.



Manques d'automatisation et d'orchestration.

7- Fonctionnalités en plus des SIEM



IA pour l'automatisation et l'orchestration

User Behavior analysis



Threat Intelligence

Analyse de la posture de
système/Réseau

Règles prédéfinies

Rétention

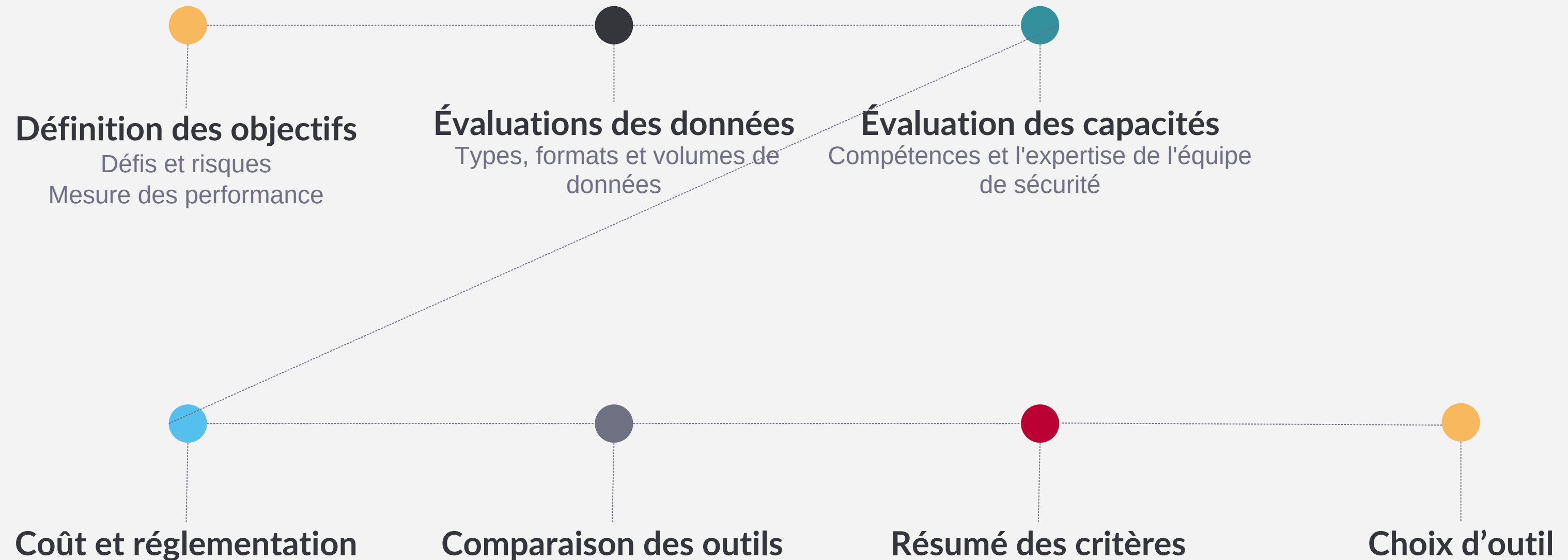


03

Partie 2 : Étude comparative

Les critères de comparaison et les différents outils
existants.

1- Démarche suivie



2- Définition des objectifs



Situation de l'ESI

Défis et risques de sécurité ?

- Les attaques liées aux infrastructures réseaux et système.
- L'espionnage et violations de données.
- Les menaces internes.

Mesure des performance de sécurité ?

- Consulter les logs des (IDS/IPS, firewall) manuellement pour détecter les anomalies.

Spécifications du SIEM

- Identifier les menaces **système et réseau**.
- Générer des alertes en **temps réel**.
- **Réponse rapide** aux incidents.
- Offrir des fonctionnalités de **forensics**.
- Surveiller les comportements des **utilisateurs internes**.
- **Intégration** avec d'autre outils de sécurité.
- Générer automatiquement des **rapports détaillés** sur l'état de sécurité.

- **Collection et centralisation** des log des (IDS/IPS, firewall).
- **Visualisation** sophistiquée des logs.
- **Corrélation** des logs pour détecter les menaces.

3- Évaluation des données



Situation de l'ESI

Spécifications du SIEM

Types et les formats de données ?

- Une variété de log (des périphériques réseau, des systèmes, des applications, des utilisateurs et des solutions de sécurité...).
- Différents formats de données.

- Collecter, stocker et analyser les journaux de sécurité provenant de **diverses sources**.
- Accepter **different formats** de données

Quantité de données ?

En constante croissance avec l'avènement de nouveaux serveurs web

- Être dimensionné pour être capable de collecter, stocker et analyser une **quantité importante de données**.
- **Etre évolutif** et capable de s'adapter à la croissance du SI.

4- Évaluation des capacités



Situation de l'ESI

Compétences et l'expertise de l'équipe ?

- Manque de compétences spécialisées dans la gestion avancée des solutions SIEM.

Temps consacré à la maintenance de la solution ?

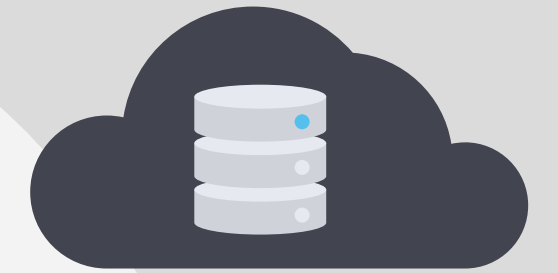
- L'équipe dispose de ressources limitées et ne peut consacrer qu'un temps limité à la maintenance du SIEM.

Spécifications du SIEM

- Support technique et **documentation** complète.
- Règles de **corrélation prédéfinies** et à jour.
- Intégrer des flux de **threat intelligence** pour enrichir les événements de sécurité avec des indicateurs de menace connus.

- **Facile à déployer** et à maintenir, avec une configuration initiale simplifiée.

5- Coût et réglementation



Situation de l'ESI

Spécifications du SIEM

Budgets associé ?

- Pas encore de budget alloué pour la solution SIEM.

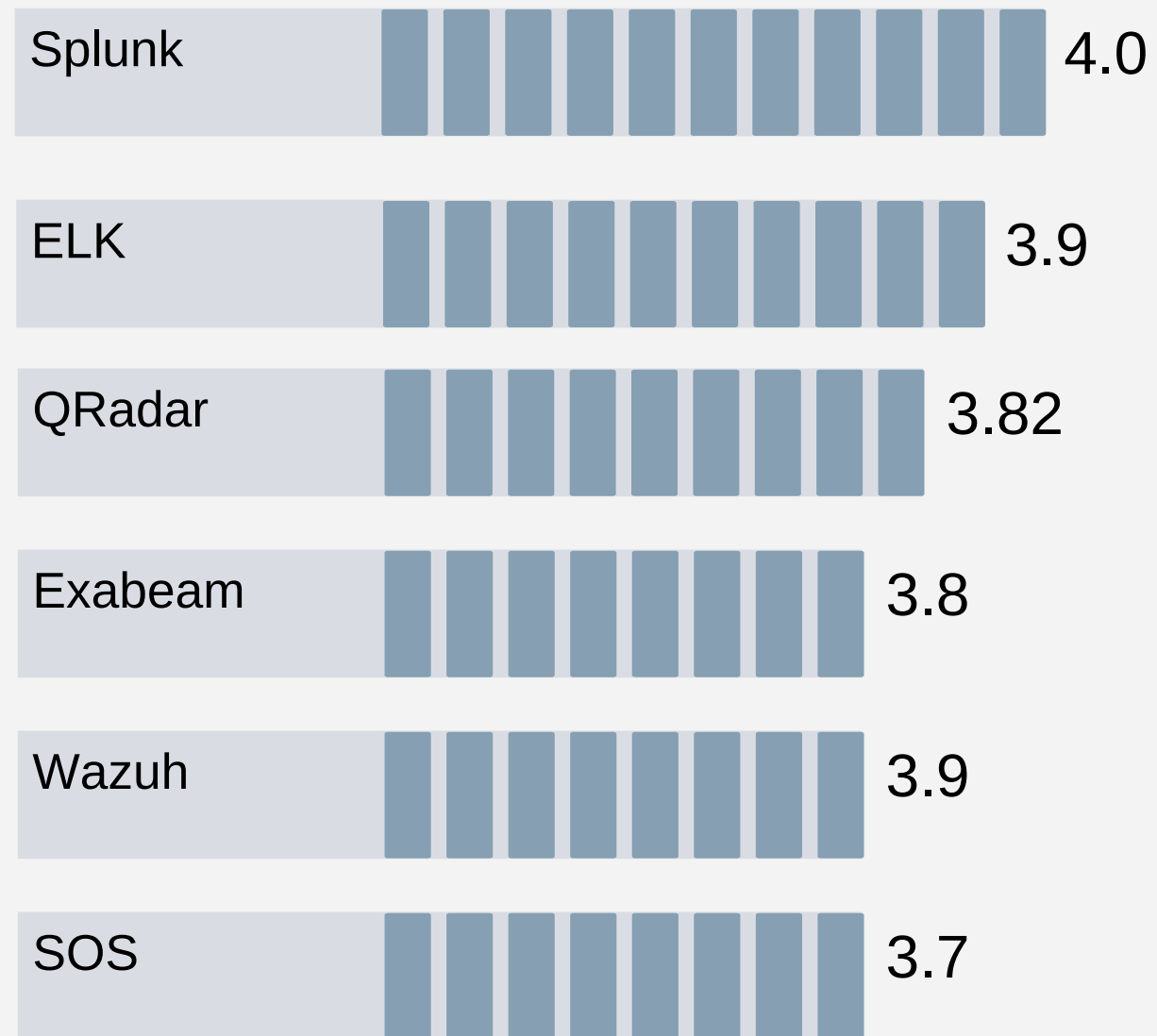
- Le SIEM doit être **open-source** et ne doit pas engendrer de coût

Normes et réglementation ?

- La conservation des données pour une période de plus de 10 ans est requise dans les établissements algériens.
Le gouvernement impose également une législation exigeant que les données des établissements publics restent sur le territoire national.

- Le SIEM doit fournir une **rétenion** des données à long terme.
Le SIEM doit fournir une solution de stockage **hors cloud**.
-

6- Outils existants



Selon Gartner

**Parmi les
meilleurs et
populaire SIEM
existants 3
d'entre eux sont
open-source et
les 3 autres sont
payantes**

7- Comparaison des outils



Splunk

Avantages

- › Surveillance en temps réel.
- › Adaptabilité à la taille de l'infrastructure.
- › Simplicité d'utilisation des fonctions de base.
- › Grande évolutivité grâce à une communauté active fournissant des add-ons et des applications.
- › Puissance du moteur d'indexation.
- › Disponibilité des règles de corrélation prédéfinies.
- ›

Inconvénients

- › Coût associé au traitement des données par gigaoctet.

7- Comparaison des outils



QRadar

Avantages

- › Corrélation d'événements sophistiqués (réduction des faux positifs).
- › Analyse des données automatisée et une visualisation rapide des menaces.
- › Génération des rapports détaillés répondant aux exigences réglementaires.
- › Adaptabilité à la taille de l'infrastructure.
- › Possibilité d'intégration avec d'autres solutions de sécurité.

Inconvénients

- › Difficile à comprendre (documentation complexe).
- Processus de sélection de licence délicat.
- › Expertise spécialisée nécessaire pour une utilisation efficace.

7- Comparaison des outils



Avantages

- › Automatisation avancée de la détection, de l'enquête et de la réponse aux menaces (algorithmes de machine learning intégrés).
- › Analyse comportementale avancée permettant de repérer les activités suspectes des utilisateurs.
- › Interface conviviale et facile.
- › Modèle de tarification prévisible.

Inconvénients

- › Coût élevé pour les petites entreprises.
- › Complexité de déploiement initial.
- › Dépendance aux API tierces pour automatiser la réponse aux incidents.
- › Besoin de données volumineuses pour une analyse comportementale efficace.

Exabeam

7- Comparaison des outils



Avantages

- › Open source.
- › Flexibilité dans les sources de données.
- › Capacités de visualisation avancées.
- › Hautement extensible, facilité d'intégration avec d'autres outils de sécurité.

Inconvénients

- › Complexité de l'implémentation et de la maintenance.
- › Problèmes de stabilité, des pannes de service et des performances peuvent survenir.
- › Absence de règles de corrélation prédéfinies.

ELK

7- Comparaison des outils



Avantages

- › Open source.
- › Système de détection d'intrusion basé sur l'hôte (HIDS).
- › Détection avancée des menaces avec une réponse automatisée aux incidents.
- › Génération des alertes en temps réel.
- › Facilité d'intégration avec d'autres outils de sécurité.
- › Disponibilité de règles de corrélation pré-définies.
- › Analyse comportementale des utilisateurs(UEBA).

Inconvénients

- › Gestion complexe des notifications en cas de volume élevé.

Wazuh

7- Comparaison des outils



Avantages

- › Open source.
- › Solution de surveillance basée sur le réseau(NIDS).
- › Facilité d'intégration avec d'autres outils de sécurité.
- › Capture complète des paquets envoyés sur le réseau.

Inconvénients

- › Complexité de l'implémentation et de la maintenance.
- › Exigences matérielles et de stockage élevées.

Security Onion

Critère en terme de sécurité



	Splunk	QRadar	Exabeam	ELK	Wazuh	SOS
Réponse aux incidents	✓	✓	✓	✗	✓	✓
Génération des alertes en temps réel	✓	✓	✓	✓	✓	✓
Intégration avec des outils de sécurité	✓	✓	✓	✓	✓	✓
Analyse de la posture de sécurité du système	✓	✓	✓	✗	✓	✗
Analyse de la posture de sécurité du réseau.	✓	✓	✓	✗	✗	✓
Corrélation sophistiqué et réduction des faux positifs	✗	✓	✓	✗	✗	✗
Performance (Rapidité, Indexation)	✓	✓	✓	✗	✓	✓
	6/7	7/7	7/7	2/7	5/7	5/7

Critères en termes de données



	Splunk	QRadar	Exabeam	ELK	Wazuh	SOS
Sources de données divers						
Gros volume de données						
Règles de corrélations personnalisable						
Scalabilité						
	4/4	4/4	4/4	4/4	3/4	4/4



Critère en terme de capacité

	Splunk	QRadar	Exabeam	ELK	Wazuh	SOS
Documentation	✓	✗	✓	✓	✓	✓
Règles de corrélation prédéfinies et à jour.	✓	✓	✓	✗	✓	✓
Intégration de la threat intelligence	✓	✓	✓	✗	✓	✗
Complexité	✗	✗	✗	✓	✗	✗
Visualization personnalisé	✓	✓	✓	✓	✓	✗
Génération de rapports	✓	✓	✓	✓	✓	✗
	5/6	4/6	5/6	4/6	5/6	2/6



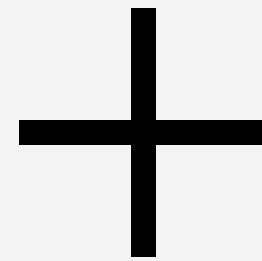
Critère en terme de coût et réglementation

	Splunk	QRadar	Exabeam	ELK	Wazuh	SOS
Coût						
Solution hors cloud						
Rétention						
	2/3	2/3	2/3	3/3	2/3	2/3
TOTAL	17/20	17/20	18/20	13/20	15/20	13/20

8- Choix d'outils



Solution 1



8- Choix d'outils



Solution 2



Security @nion



elastic

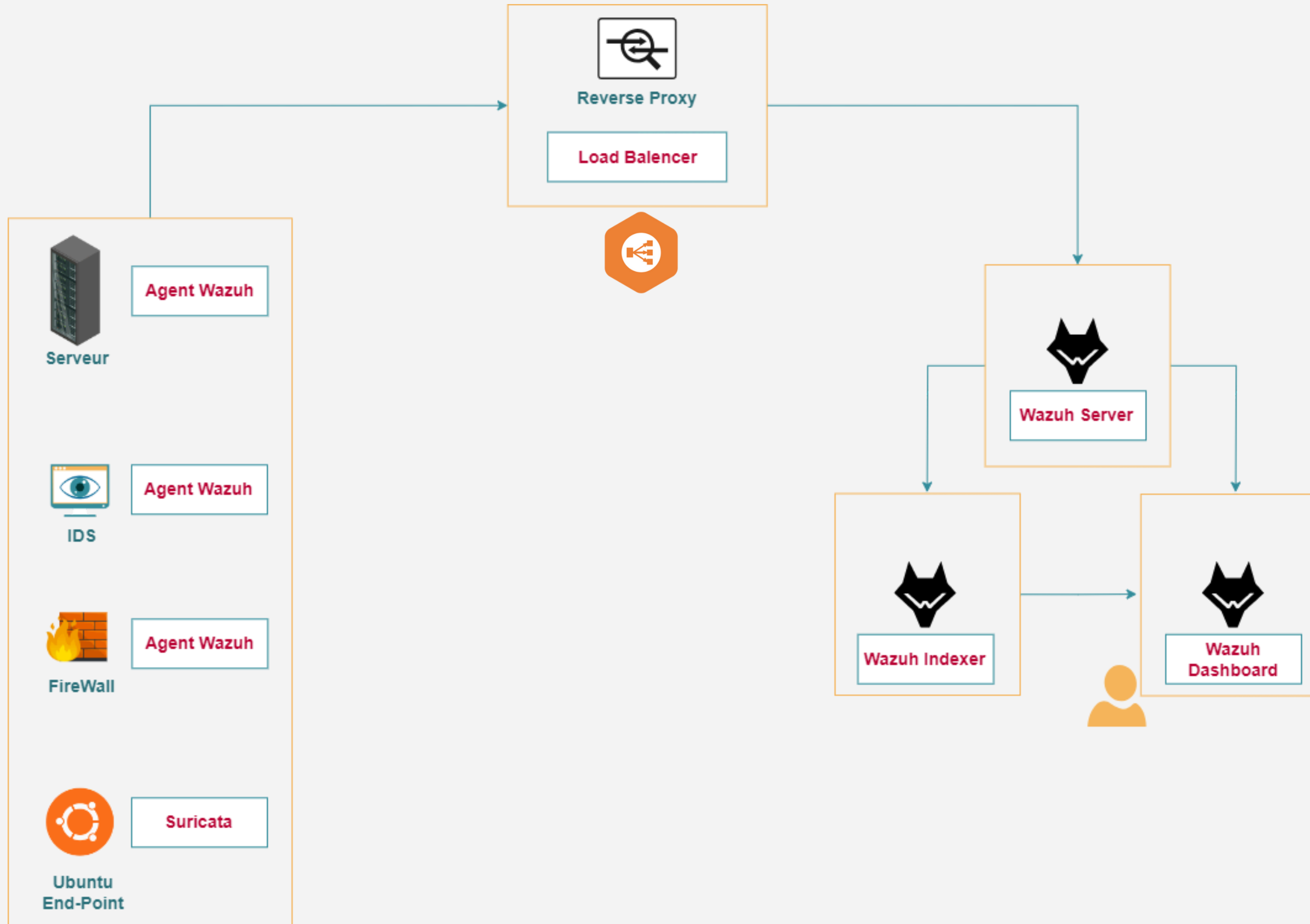


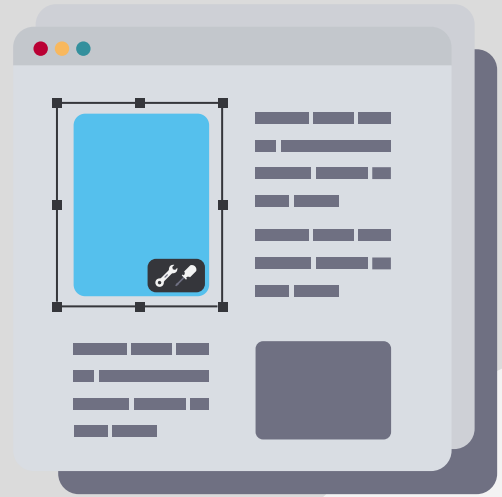
04

Solution choisie

Architecture de notre solution.

Solution Proposée





Merci !

