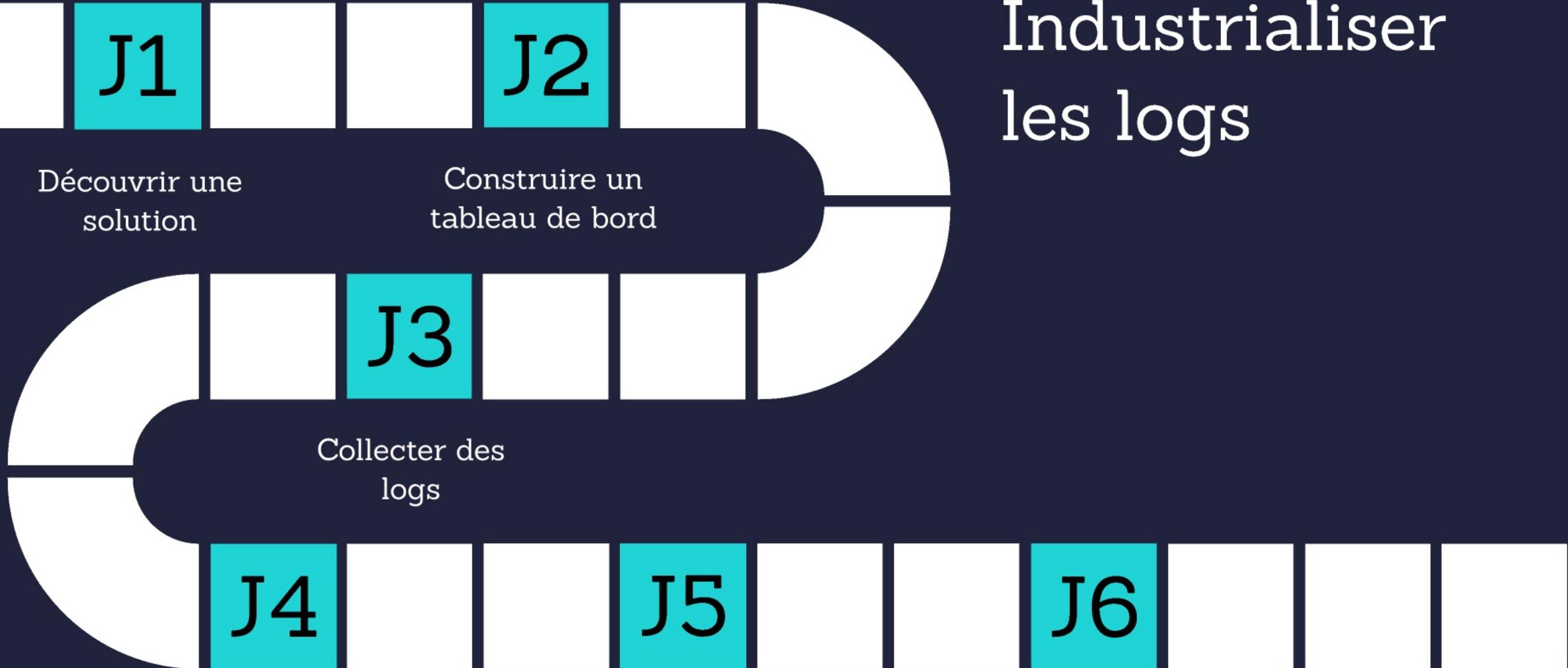


Industrialiser les logs



Transformer
des logs

Déployer des
collecteurs

Alerter

Découvrir une solution

Présentation de Nicolas

Tour de table

Objectifs de la formation

Modalités d'évaluation des acquis

Introduction à
l'industrialisation
de logs

Installer
une
solution

Remplir le
formulaire

Introduction à l'industrialisation de logs

1 Qu'est ce qu'un log ?

2 Pourquoi centraliser les logs ?

3 Qu'est-ce que l'Observabilité ?

4 Quelles solutions pour centraliser les logs ?

5 Qu'est-ce que la stack Elastic ?

6 Qu'est-ce que l'industrialisation de logs ?



Découvrir une solution

Présentation de Nicolas

Tour de table

Objectifs de la formation

Modalités d'évaluation des acquis

Introduction à
l'industrialisation
de logs

Installer
une
solution

Remplir le
formulaire

Formulaire

<https://forms.gle/nEc8UumdN619EGXJ6>



Découvrir une solution

Présentation de Nicolas

Tour de table

Objectifs de la formation

Modalités d'évaluation des acquis

Introduction à
l'industrialisation
de logs

Installer
une
solution

Remplir le
formulaire

Installer la stack Elastic

En local sur vos postes

1 Installer Elasticsearch

2 Installer Kibana

Découvrir une solution

Présentation de Nicolas

Tour de table

Objectifs de la formation

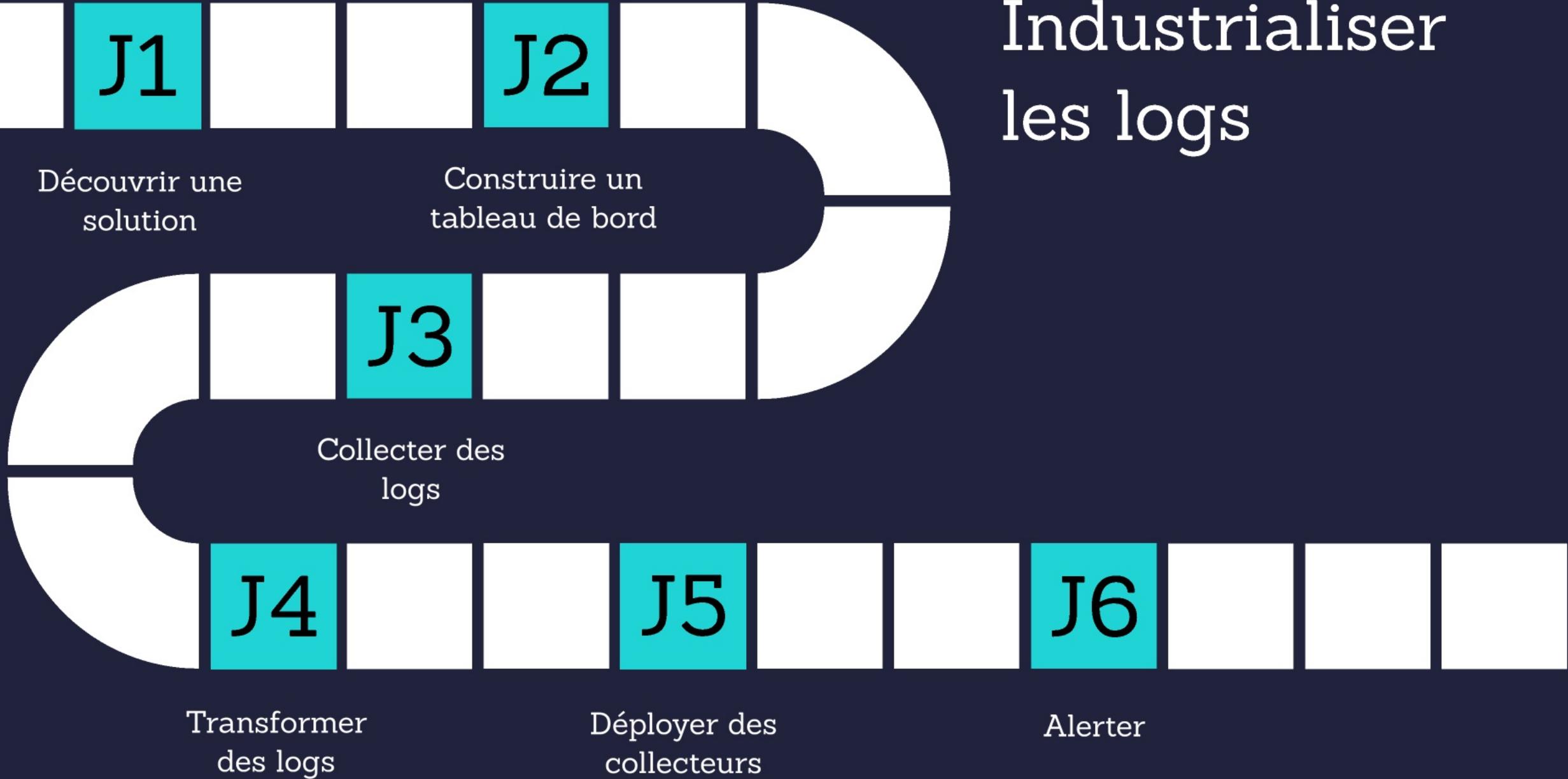
Modalités d'évaluation des acquis

Introduction à
l'industrialisation
de logs

Installer
une
solution

Remplir le
formulaire

Industrialiser les logs



Construire un tableau de bord

Analyser les données

Choisir les éléments graphiques

Agencer le tableau de bord

Kibana

Kibana
sample data
logs

Réponses au
formulaire
J1

Kibana

1 Discover

2 Visualize

3 Dashboard

Construire un tableau de bord

Analyser les données

Choisir les éléments graphiques

Agencer le tableau de bord

Kibana

Kibana
sample data
logs

Réponses au
formulaire
J1

Dashboard à partir du csv

3 types de graphique différents

Construire un tableau de bord

Analyser les données

Choisir les éléments graphiques

Agencer le tableau de bord

Kibana

Kibana
sample data
logs

Réponses au
formulaire
J1

Construire 3 visu pour l'analyse des logs du site elastic.co

Clientip unique

Code retour

Machine OS

Combien d'utilisateurs différents ont visité le site ?

Les visiteurs ont-ils rencontré des erreurs ?

Quel est l'OS des visiteurs ?

Requête HTTP

Requête par heure

Accès externe

Top 5 des requêtes HTTP
(Horizontal bar chart)

Nombre de requête par heure de la journée

Accès ne provenant pas de elastic-elastic-elastic.com

Construire un tableau de bord

Analyser les données

Choisir les éléments graphiques

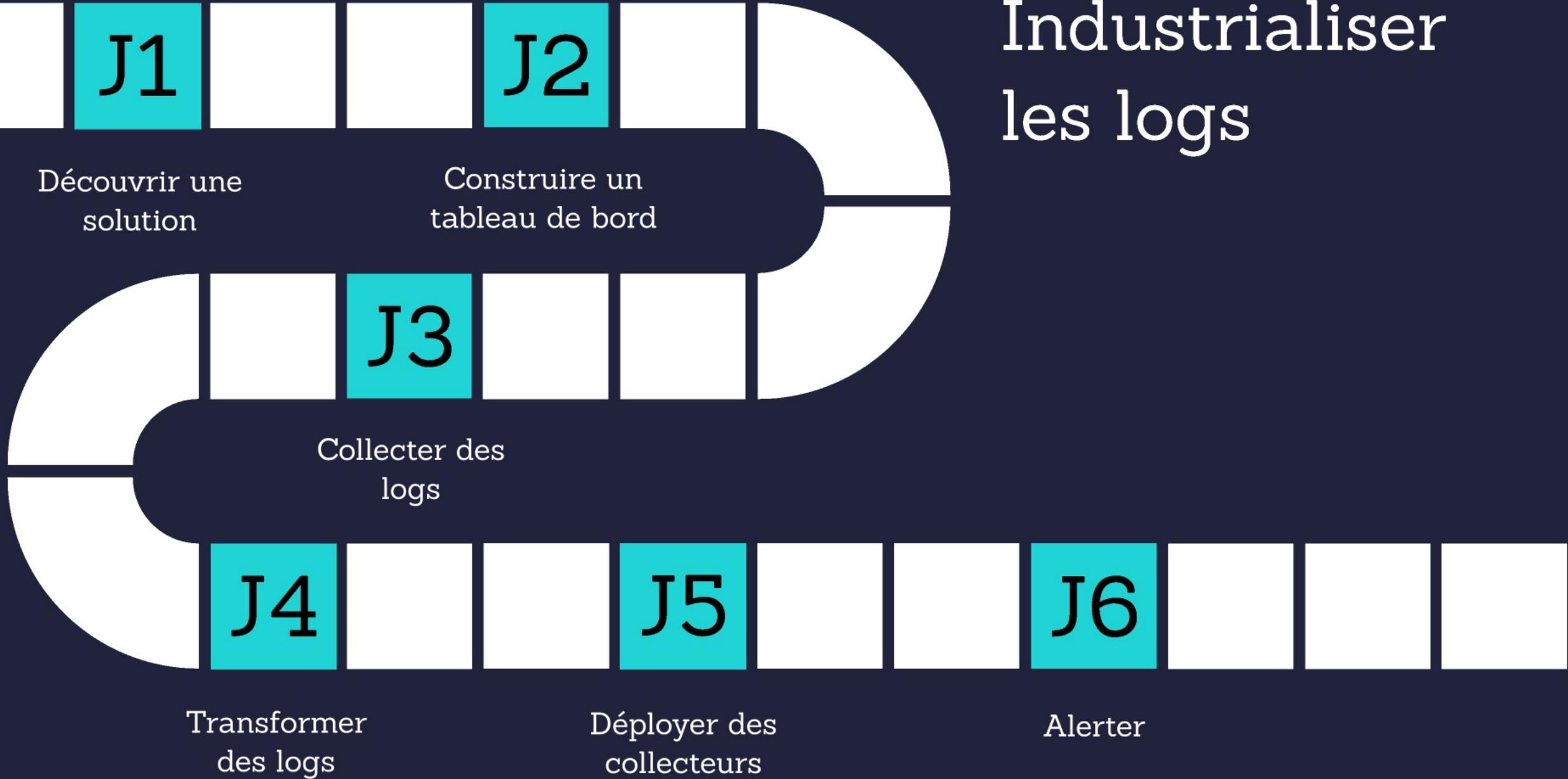
Agencer le tableau de bord

Kibana

Kibana
sample data
logs

Réponses au
formulaire
J1

Industrialiser les logs



Collecter des logs

Apache access log

(Postgres database)

Filebeat

Logstash

Elasticsearch

Filebeat

Installer Filebeat en local

Configurer Filebeat

Collecter des logs

Apache access log

(Postgres database)

Filebeat

Logstash

Elasticsearch

Logstash

1 Input

2 Filter

3 Output

Collecter des logs

Apache access log

(Postgres database)

Filebeat

Logstash

Elasticsearch

Elasticsearch



Index vs. Datastream
Sharding



ILM
Rétention



Index & Component template
Mapping, Settings



Ingest pipelines vs. Logstash
Kafka



Logstash centralized pipeline
management



Monitoring

Collecter des logs

Apache access log

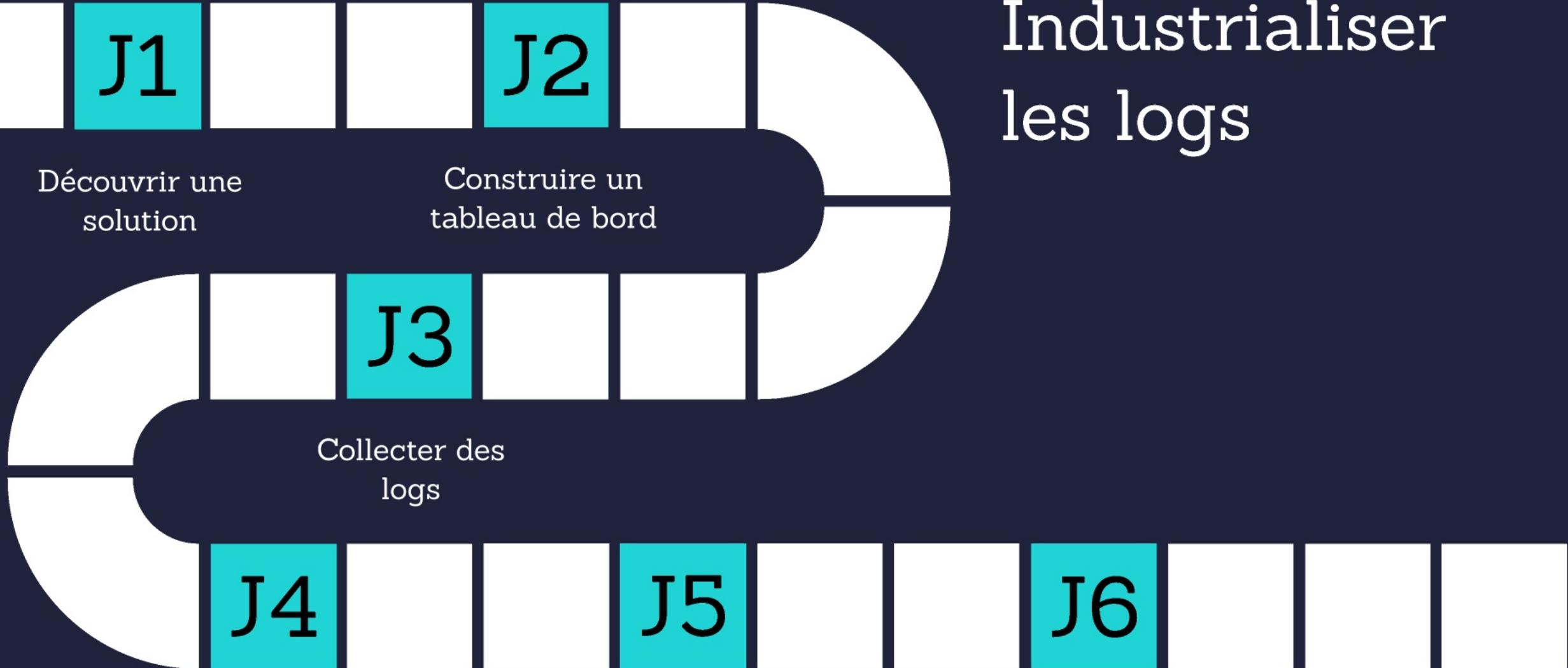
(Postgres database)

Filebeat

Logstash

Elasticsearch

Industrialiser les logs



Transformer
des logs

Déployer des
collecteurs

Alerter

Log parsing

Traiter les données pendant la collecte pour faciliter leur manipulation ultérieure

Logstash

Fleet

Ingest
Pipeline

Logstash

Log parsing

Traiter les données pendant la collecte pour faciliter leur manipulation ultérieure

Logstash

Fleet

Ingest
Pipeline

Ingest Pipeline

Log parsing

Traiter les données pendant la collecte pour faciliter leur manipulation ultérieure

Logstash

Fleet

Ingest
Pipeline

Fleet

Log parsing

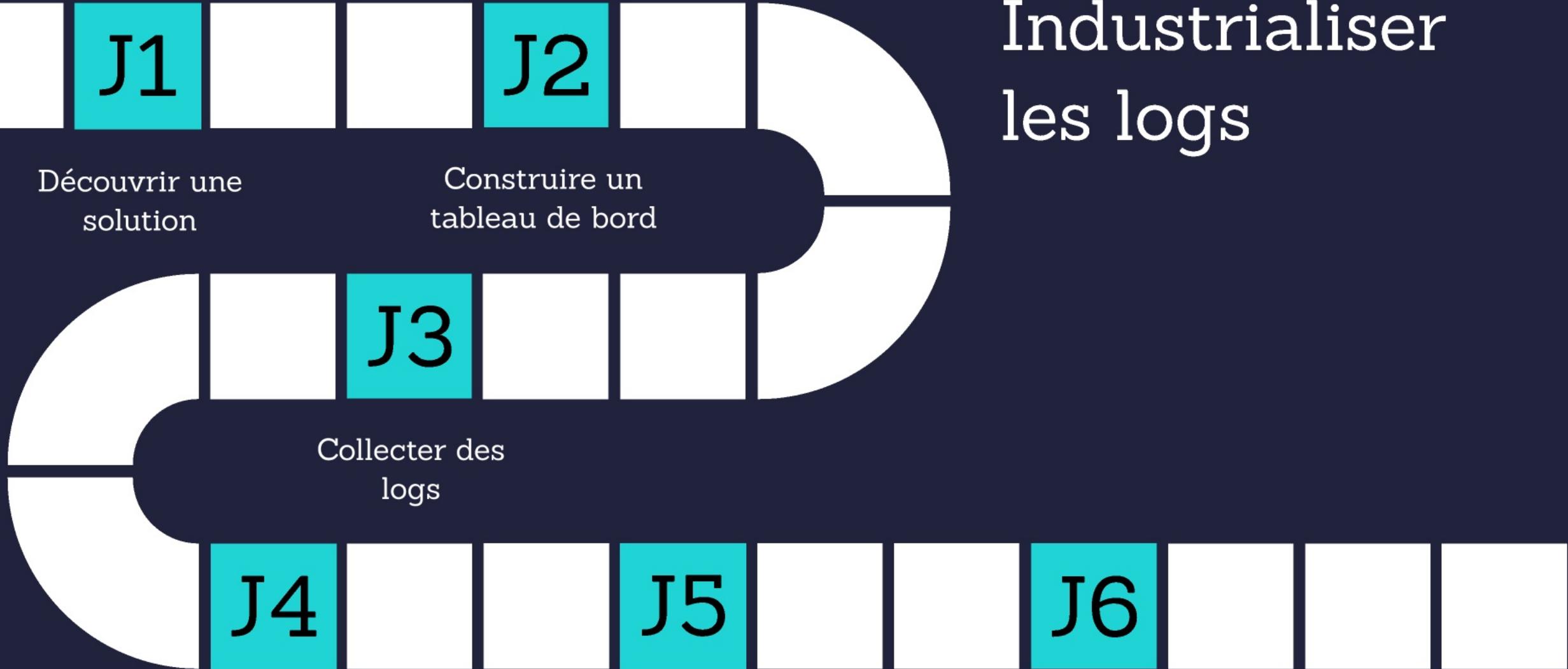
Traiter les données pendant la collecte pour faciliter leur manipulation ultérieure

Logstash

Fleet

Ingest
Pipeline

Industrialiser les logs



Transformer
des logs

Déployer des
collecteurs

Alerter

Fleet

Ajouter des intégrations à une politique

Apache log

Autres
intégration

Apache log

Ajouter l'intégration Apache log

Fleet

Ajouter des intégrations à une politique

Apache log

Autres
intégration

Autres intégrations

Ajouter d'autres intégrations à la politique

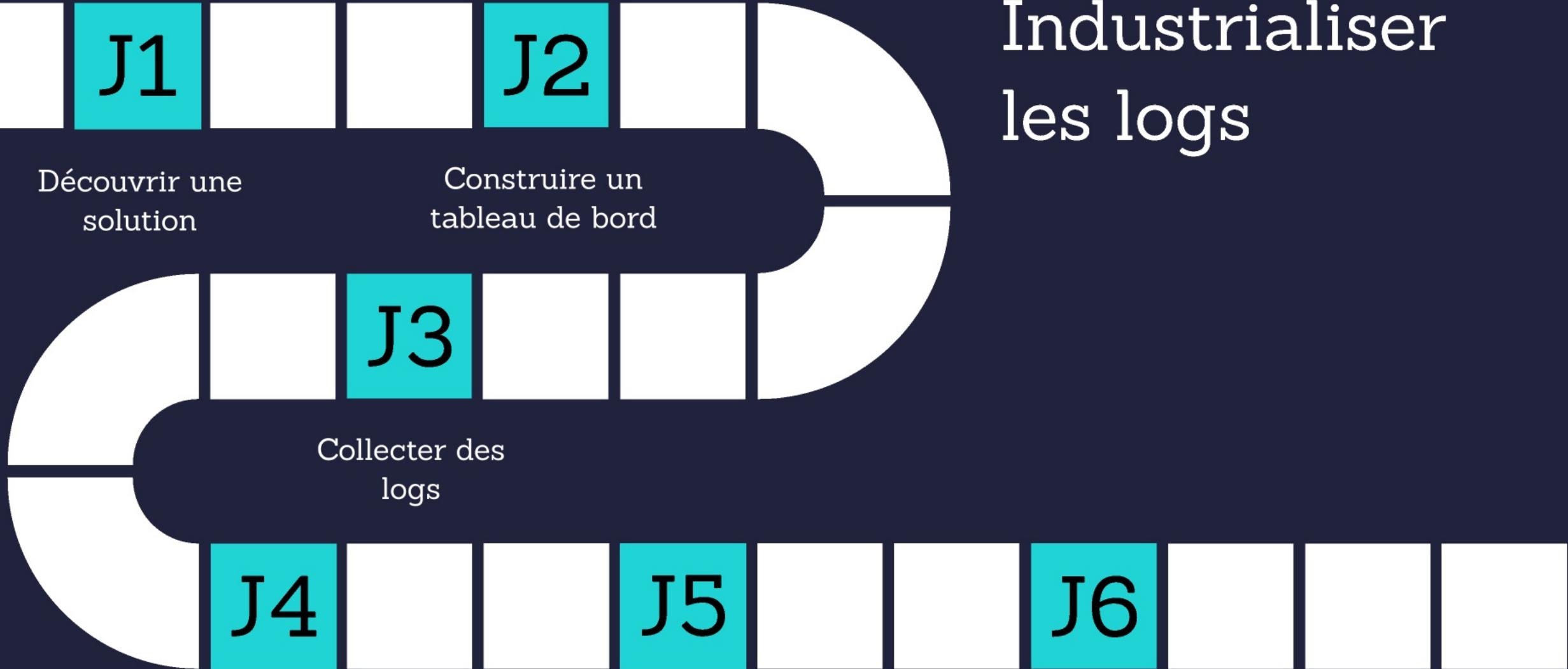
Fleet

Ajouter des intégrations à une politique

Apache log

Autres
intégration

Industrialiser les logs



Transformer
des logs

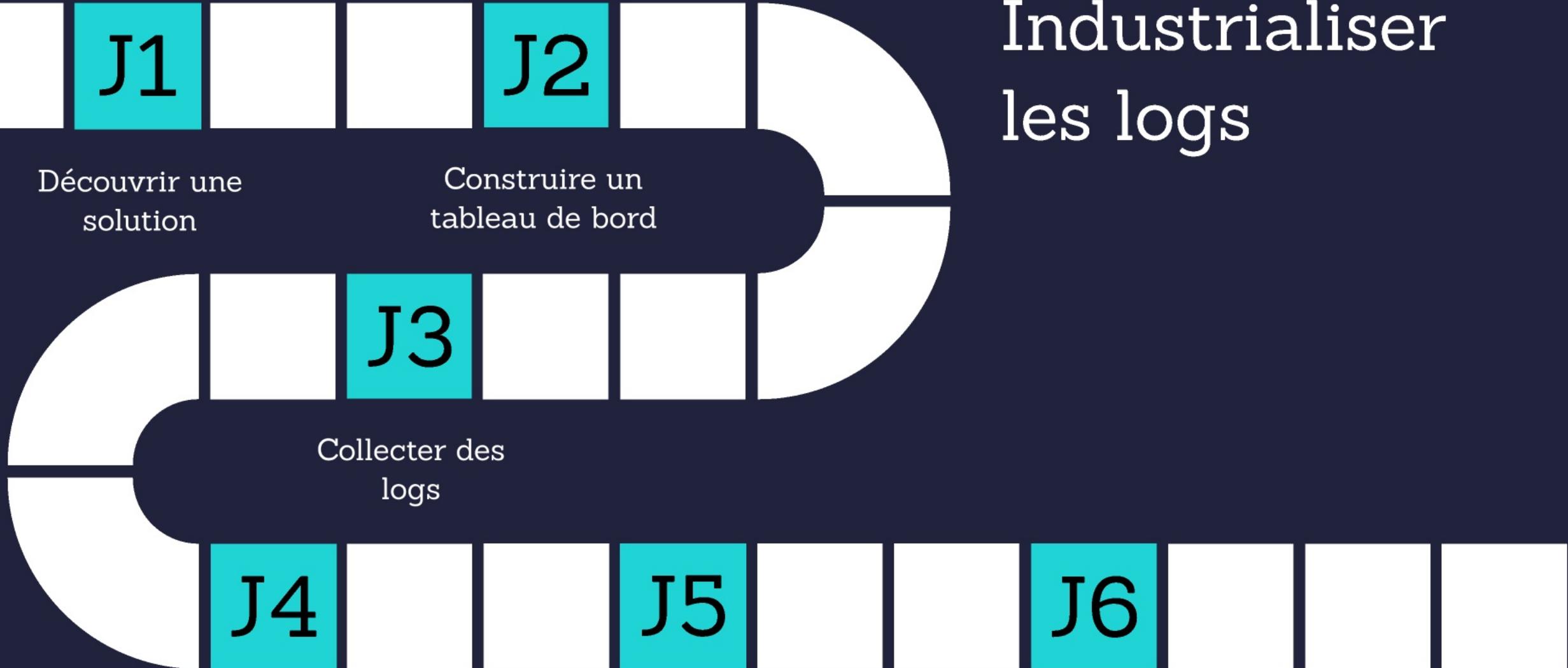
Déployer des
collecteurs

Alerter

Alerter avec Elastic

Kibana Alerting vs. Watcher

Industrialiser les logs



Transformer
des logs

Déployer des
collecteurs

Alerter

Industrialiser les logs

