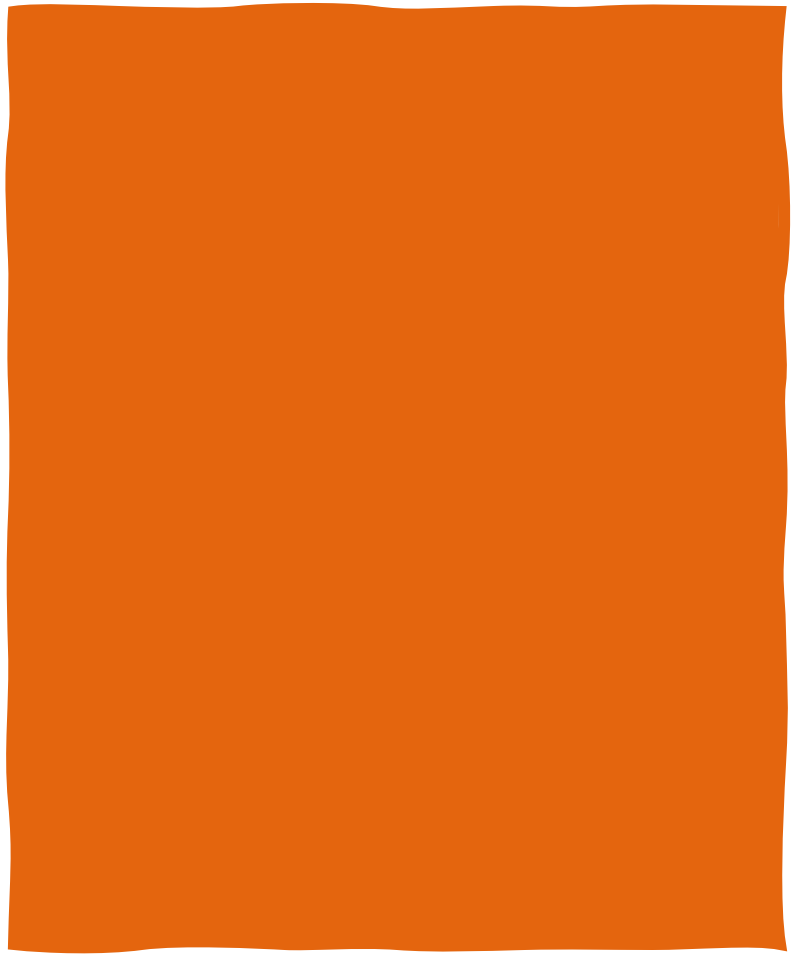
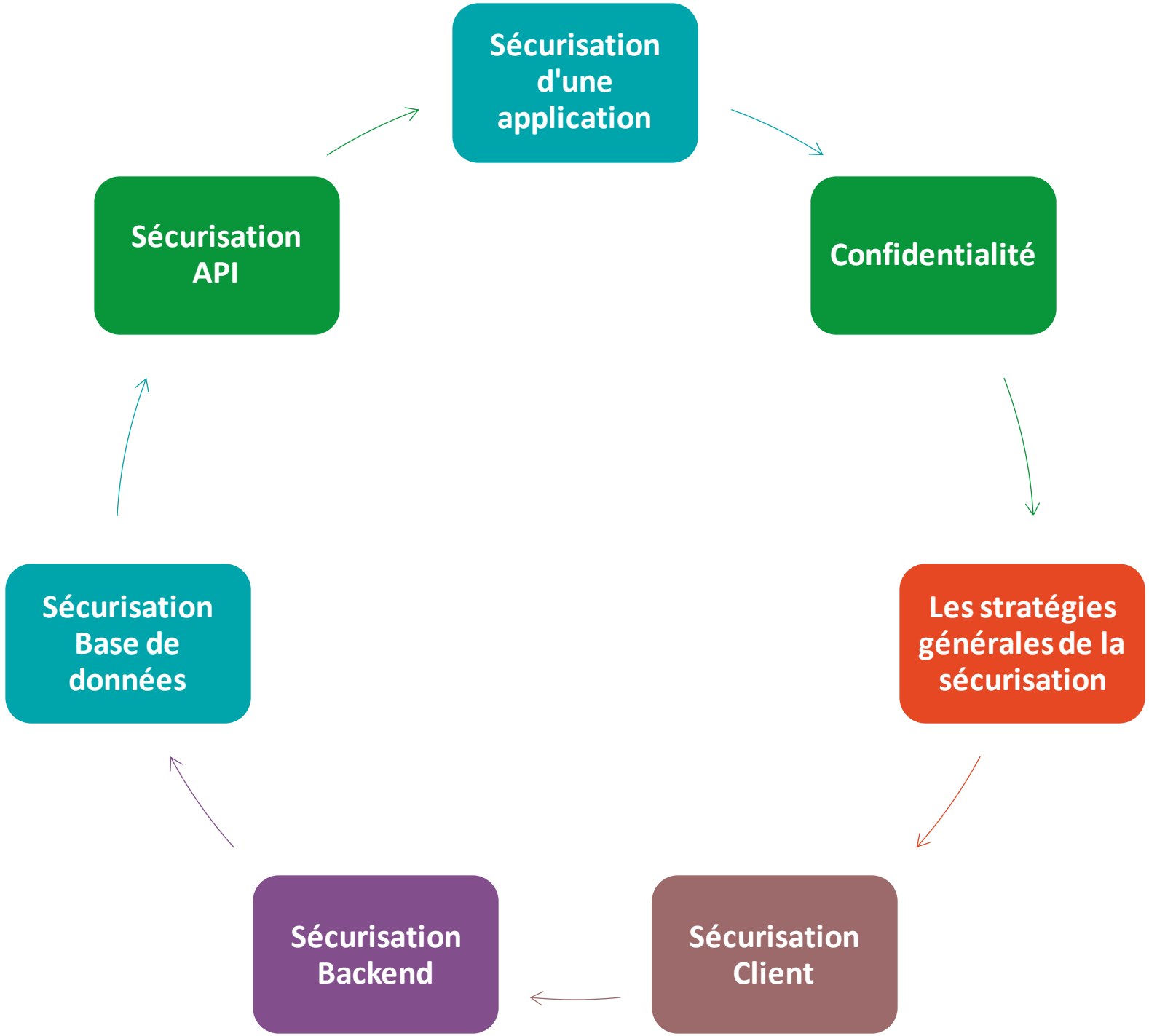
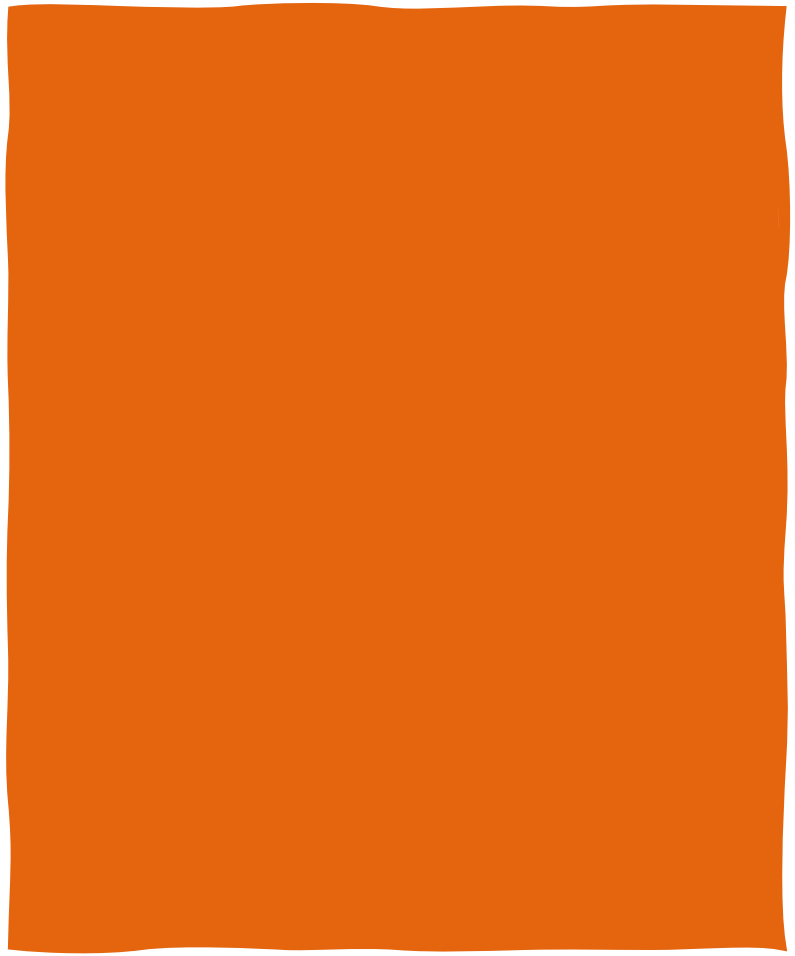
# PROPOSITION DE STRATÉGIE DE SÉCURISATION D'UNE APPLICATION



# Sommaire

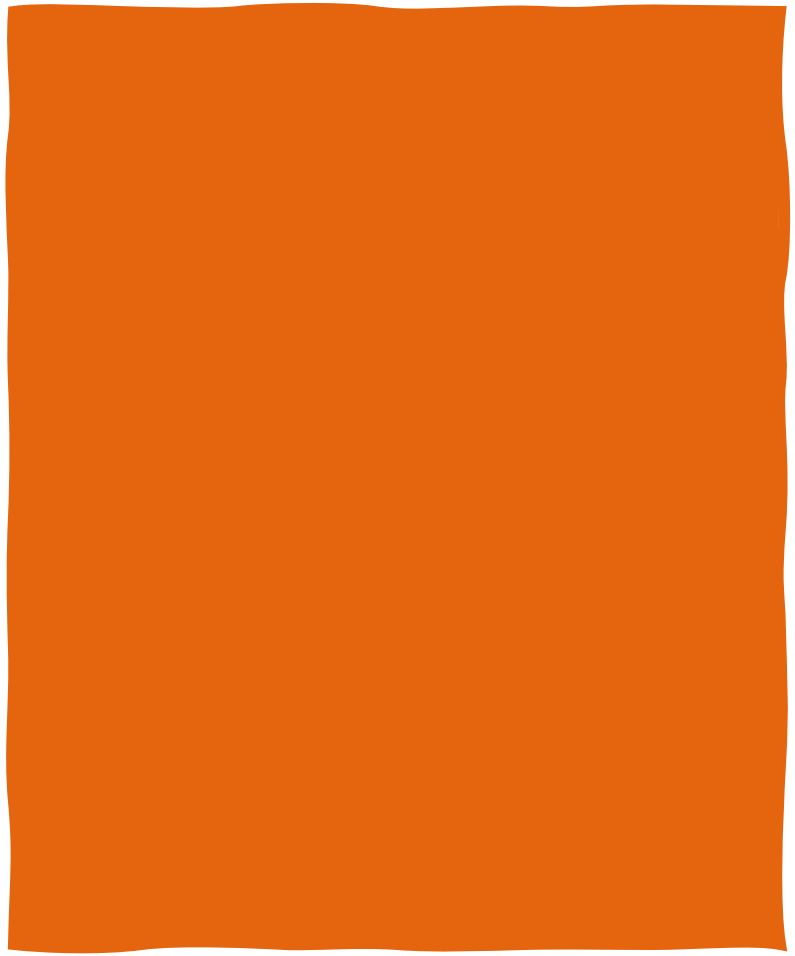

Sécurisation d'une application
Confidentialité
Les stratégies générales de la sécurisation
Sécurisation Client
Sécurisation Backend
Sécurisation Base de données
Sécurisation API

# SÉCURISATION D'UNE APPLICATION



# QUE VEUT DIRE SÉCURISER UNE APPLICATION ?

# CONFIDENTIALITÉ



RESPONSABILITÉ


TRANSPARENCE

CONFIANCE

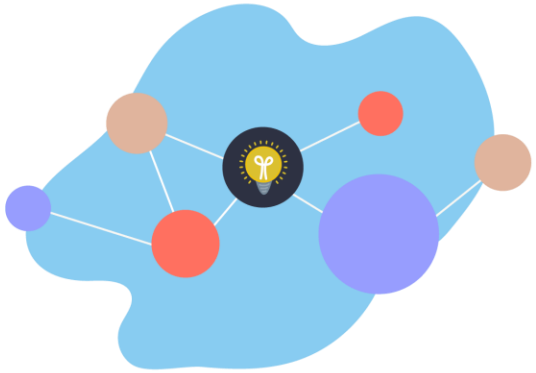
# QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

# QU'EST-CE QU'UN TRAITEMENT DE DONNÉES PERSONNELLES ?

*Les données personnelles sont traitées dès qu'elles sont...*

*Récoltées*

*Analysées*



*Utilisées*

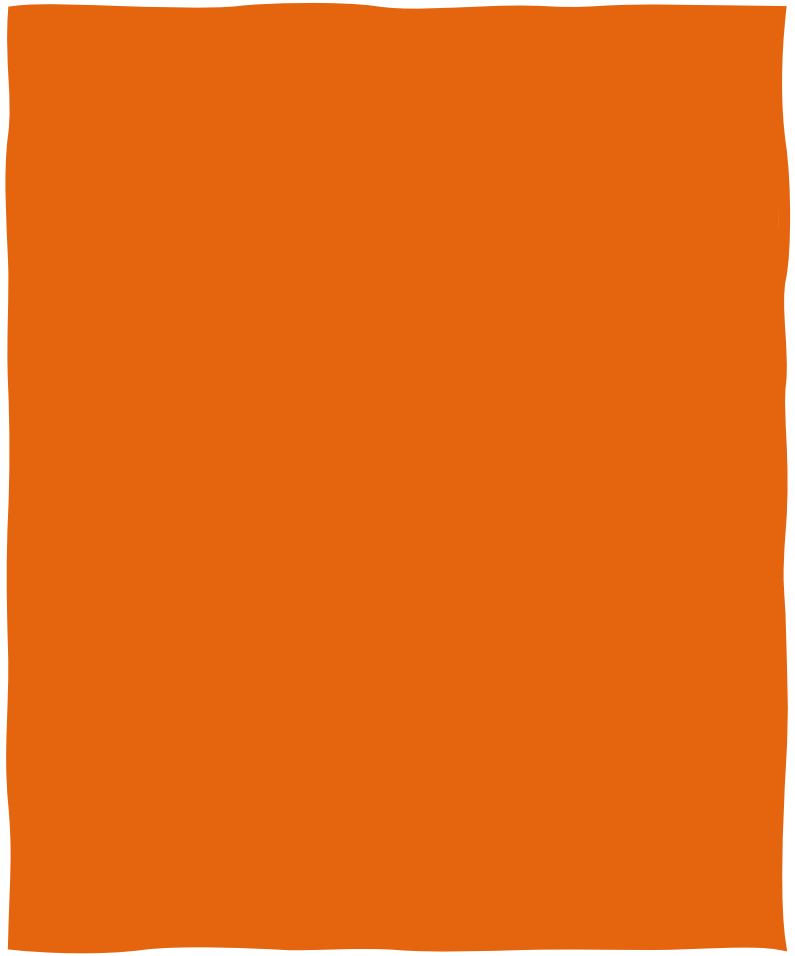
*Stockées*

reflexe CSE

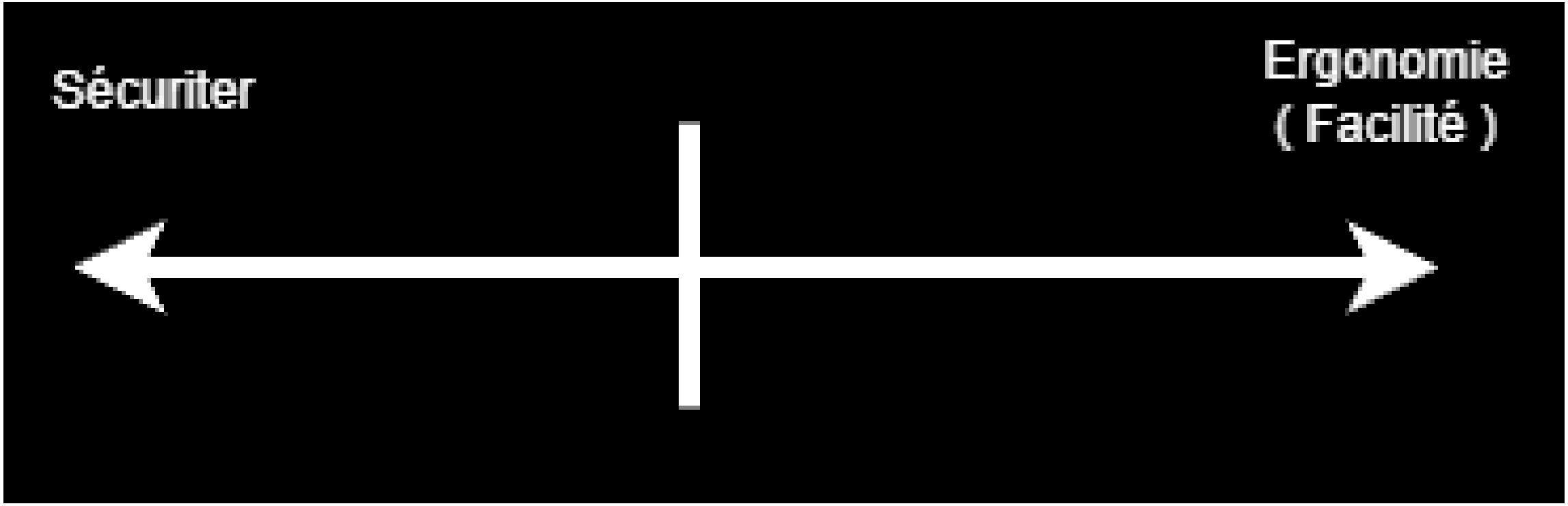
# JE PROPOSE QUE POUR VOTRE APPLICATION NOUS SUIVONS LES 5 BONS RÉFLEXES MIS EN PLACE PAR LA COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL).

- LE PRINCIPE DE FINALITÉ
- LE PRINCIPE DE PROPORTIONNALITÉ ET DE PERTINENCE
- LE PRINCIPE D'UNE DURÉE DE CONSERVATION LIMITÉE
- LE PRINCIPE DE SÉCURITÉ ET DE CONFIDENTIALITÉ
- LES DROITS DES PERSONNES

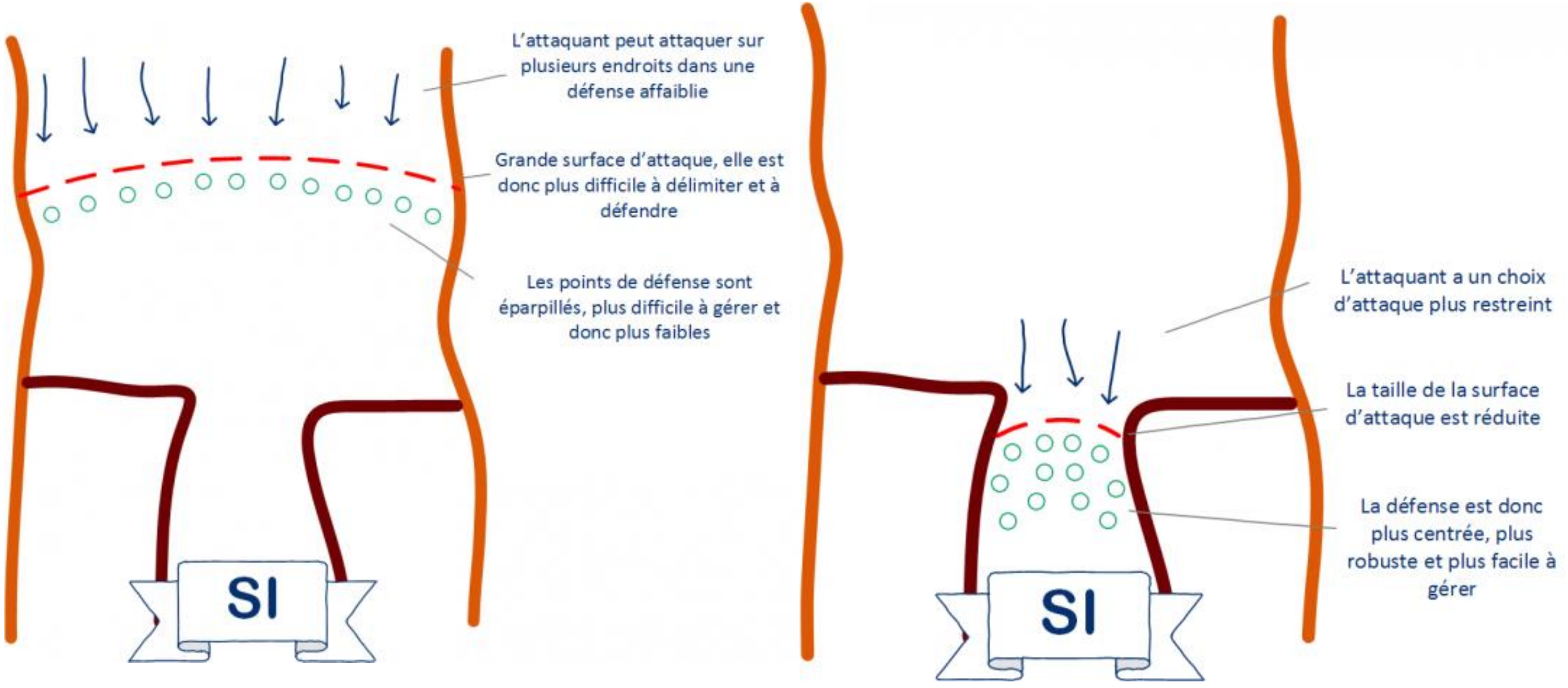
# LES STRATÉGIES GÉNÉRALES DE LA SÉCURISATION



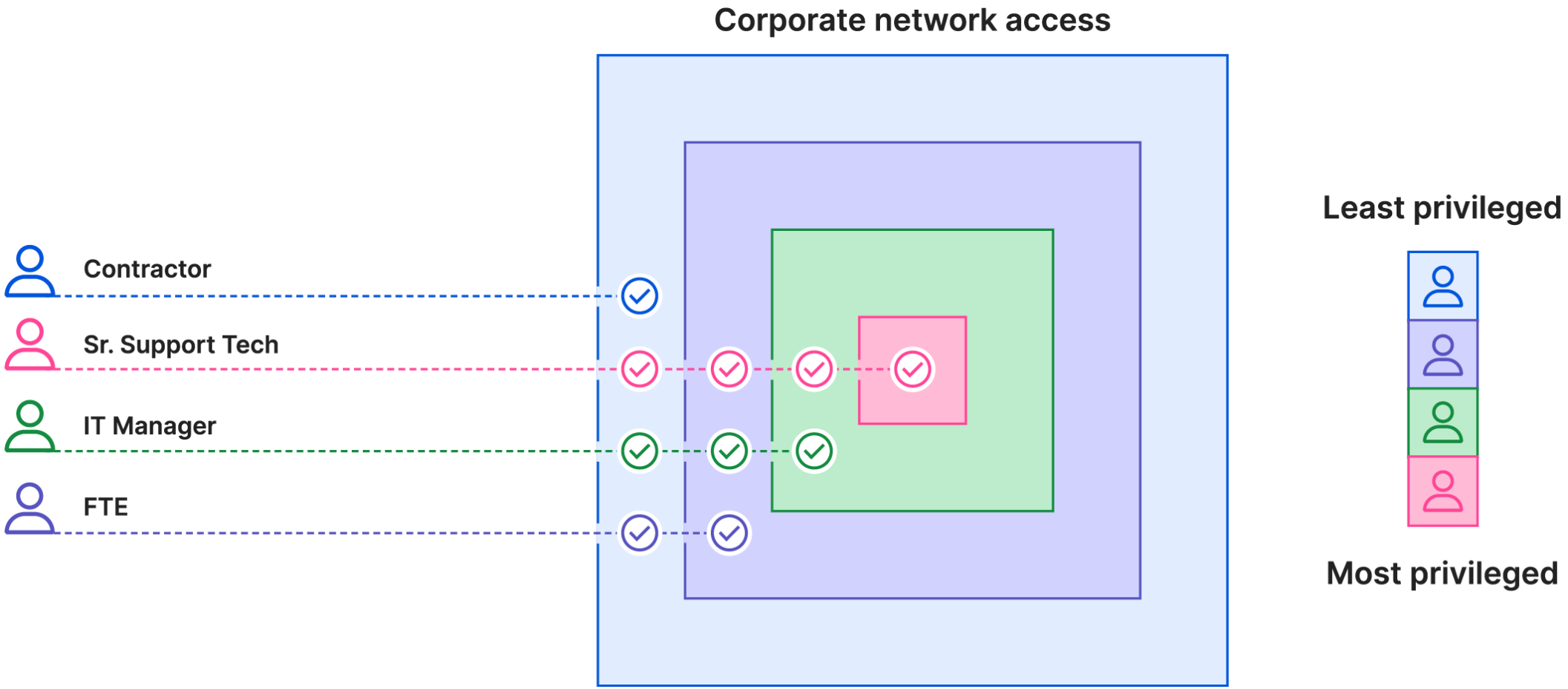
# LES STRATÉGIES GÉNÉRALES DE LA SÉCURISATION



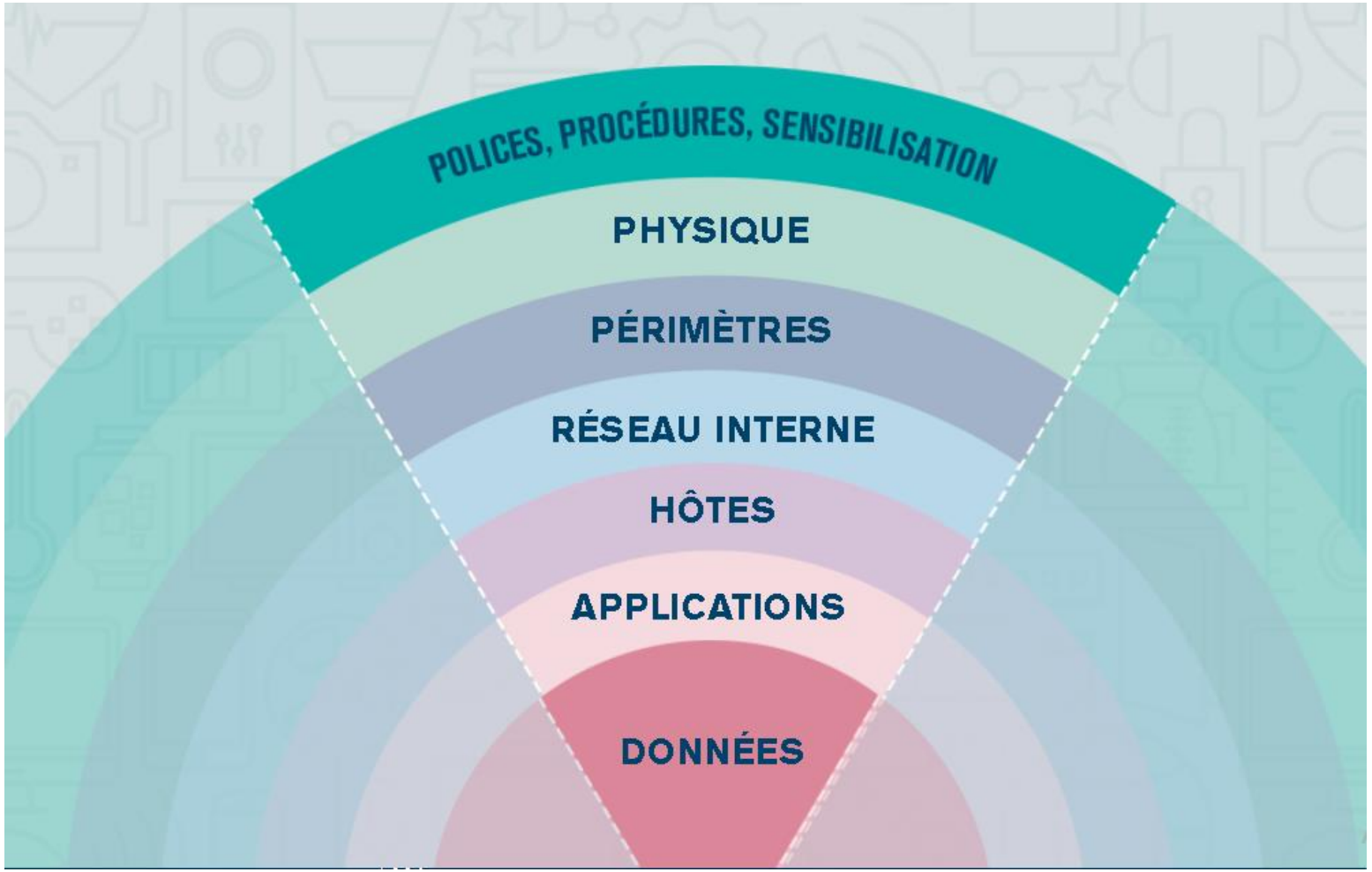
# RÉDUCTION DE LA SURFACE D'ATTAQUE



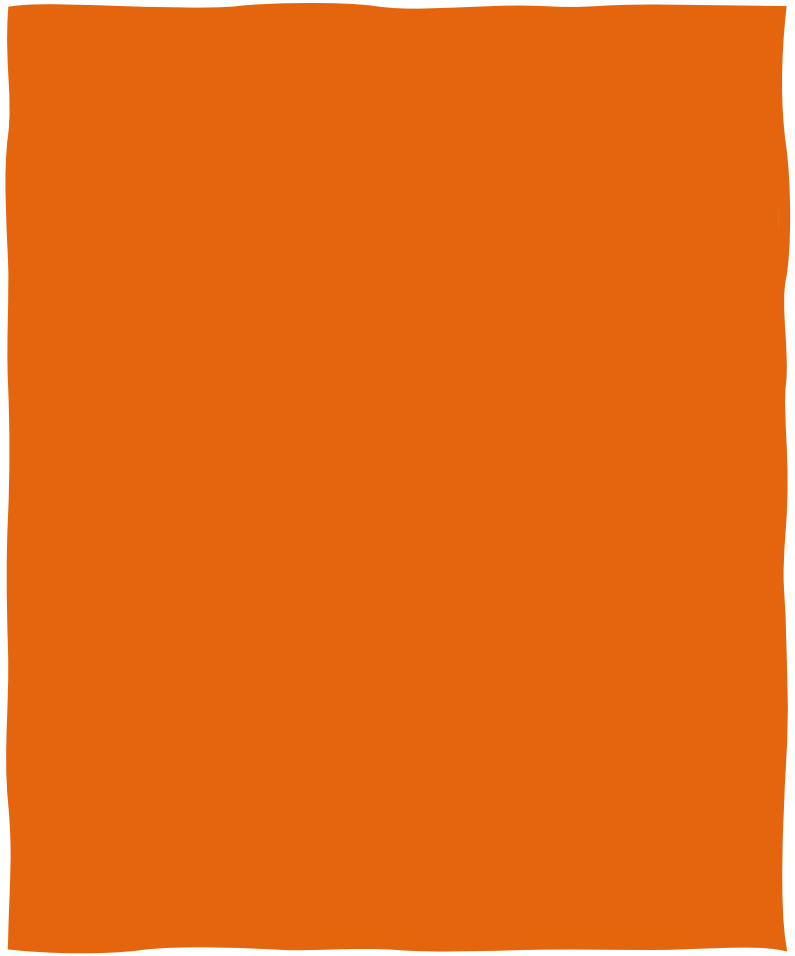
# MOINDRE PRIVILÈGE



# DÉFENSE EN PROFONDEUR



# SÉCURISATION CLIENT

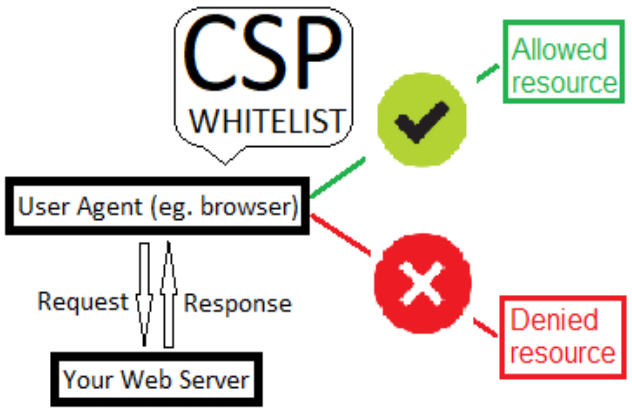


# INCLUSION SÉCURISÉE DE CONTENUS TIERS

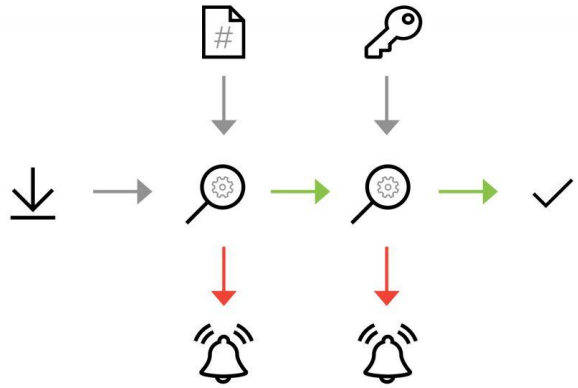
## POLITIQUE DE LA MÊME ORIGINE (SOP)

## PARTAGE DE RESSOURCES INTER-ORIGINE (CORS)

## POLITIQUE DE SÉCURITÉ DU CONTENU (CSP)




## INTÉGRITÉ DES SOUS-RESSOURCES (SRI)

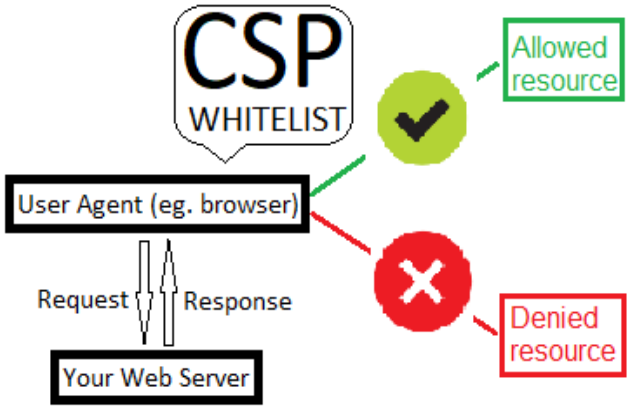


# COOKIE

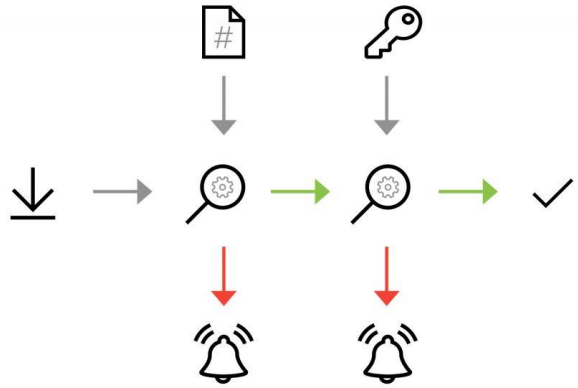
## POLITIQUE DE LA MÊME ORIGINE (SOP)

## PARTAGE DE RESSOURCES INTER-ORIGINE (CORS)

## POLITIQUE DE SÉCURITÉ DU CONTENU (CSP)

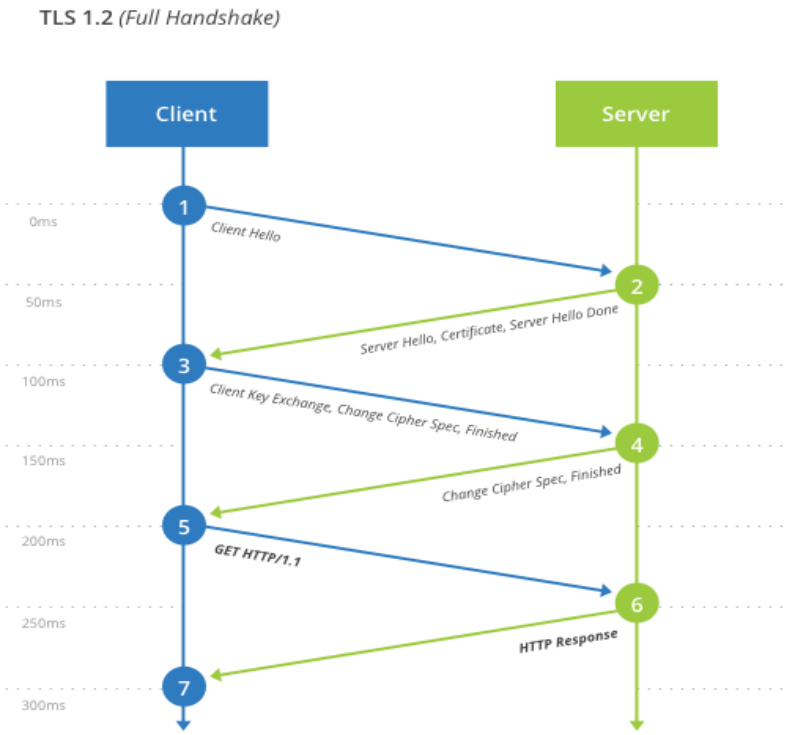



## INTÉGRITÉ DES SOUS-RESSOURCES (SRI)

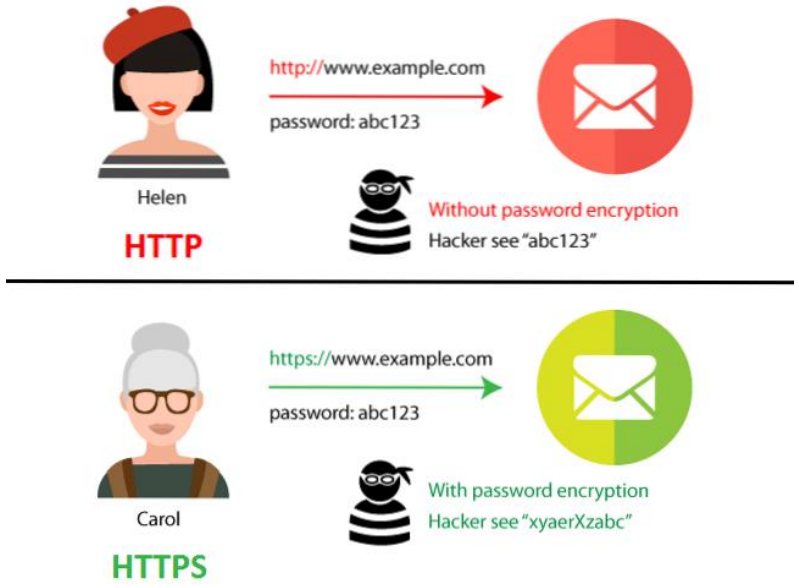


# HTTPS - TLS - HSTS

## TRANSPORT LAYER SECURITY (TLS)




## HYPER TEXT TRANSFER PROTOCOL SECURE (HTTPS)




## HYPER TEXT TRANSFER PROTOCOL SECURE (HTTPS)

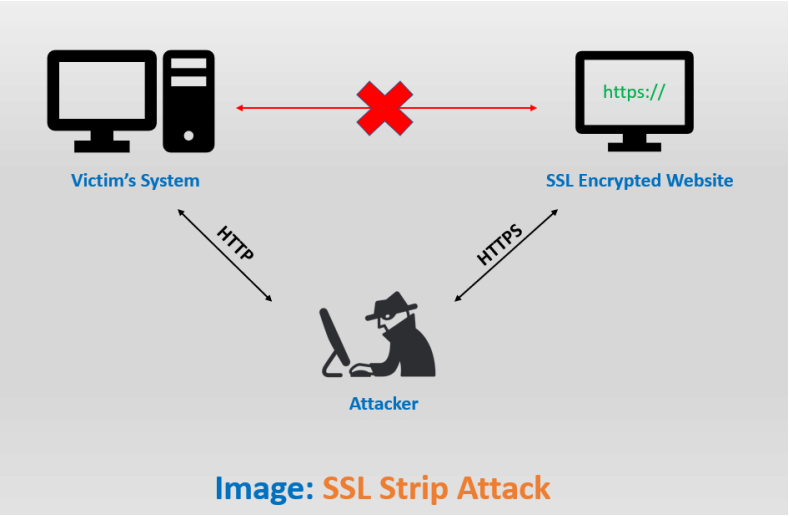
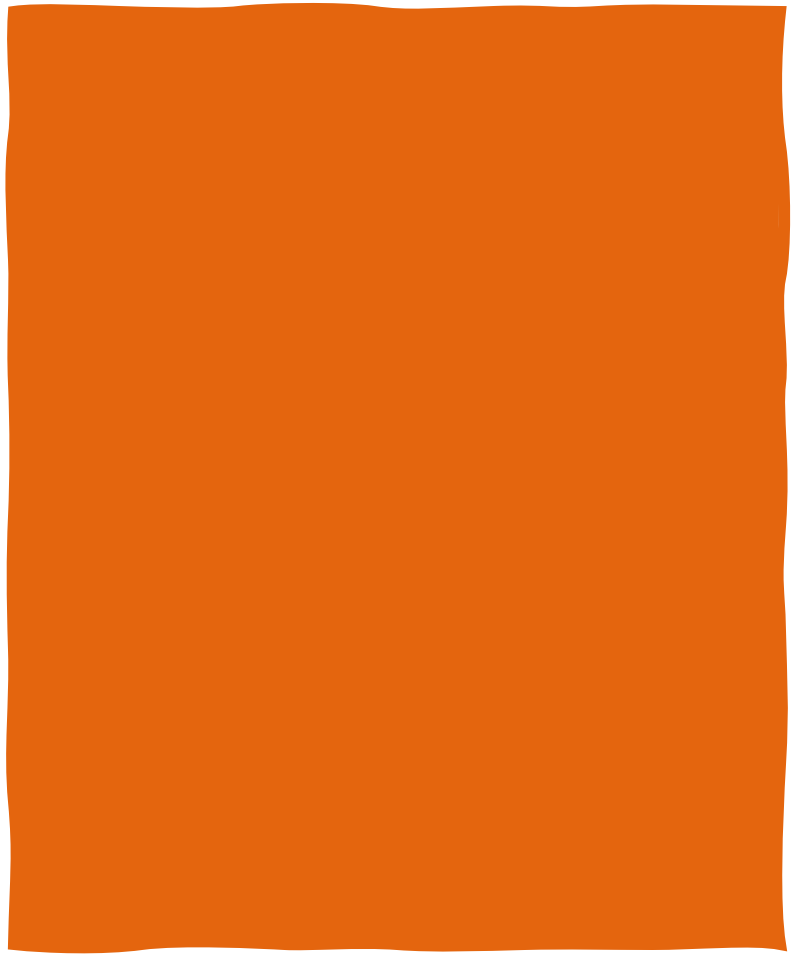
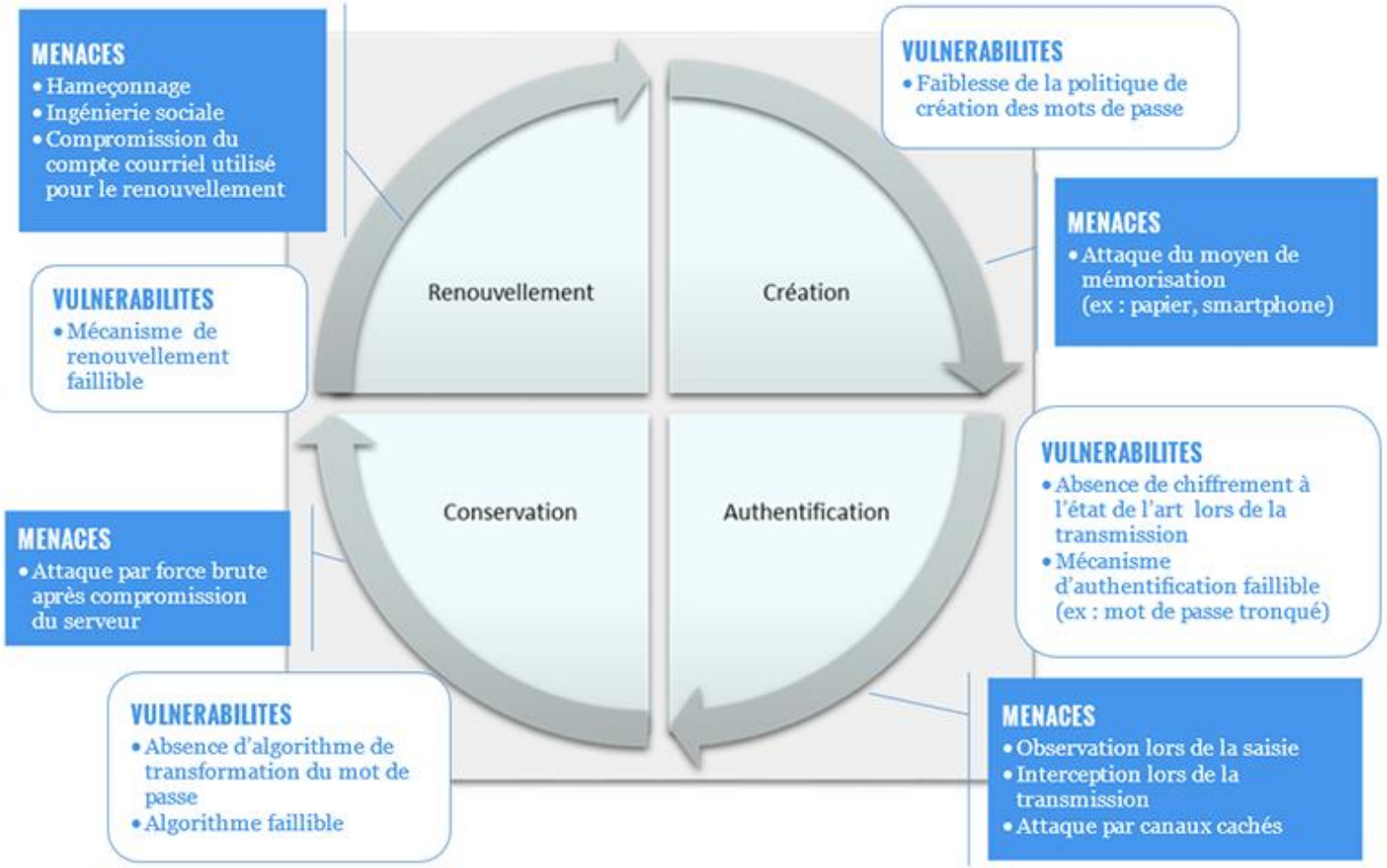



Image: SSL Strip Attack

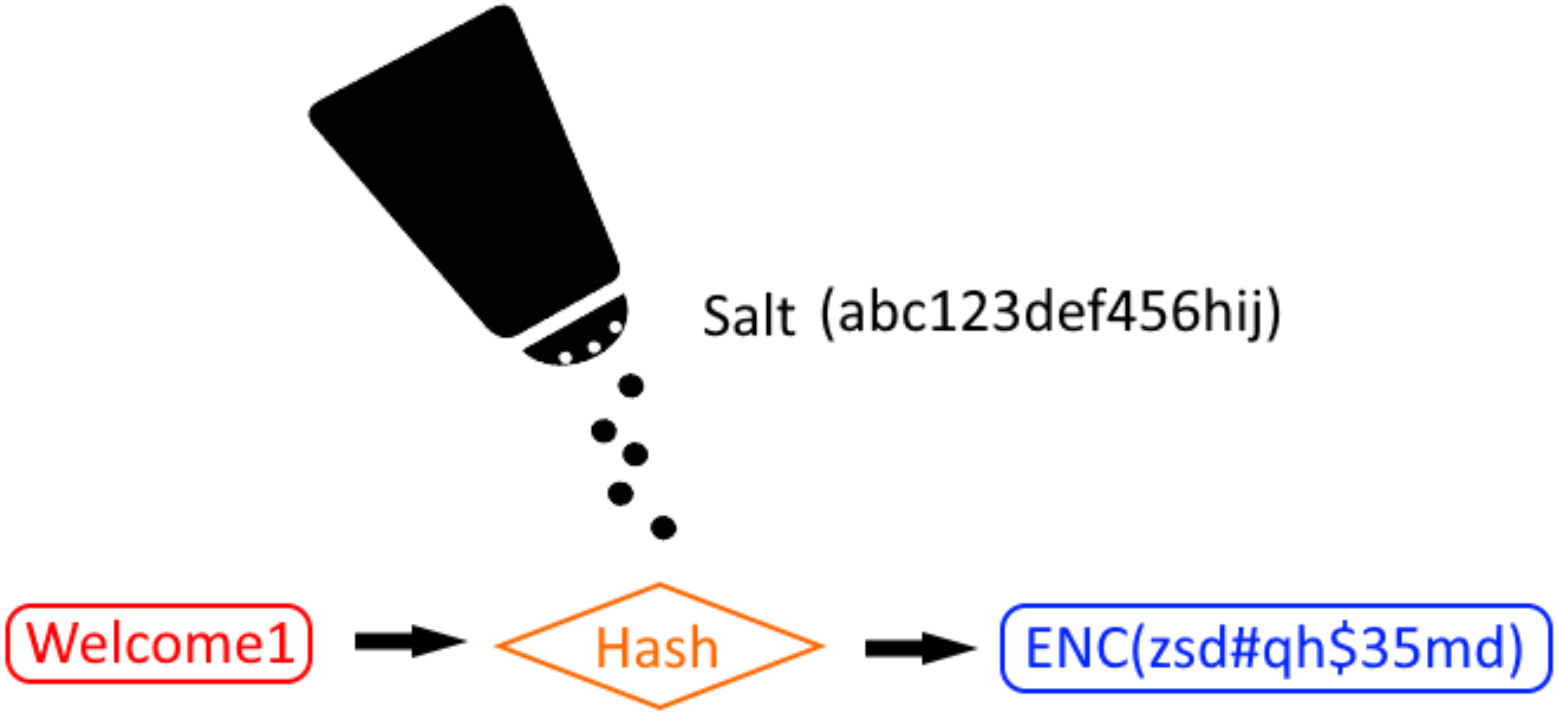
# SÉCURISATION BACKEND



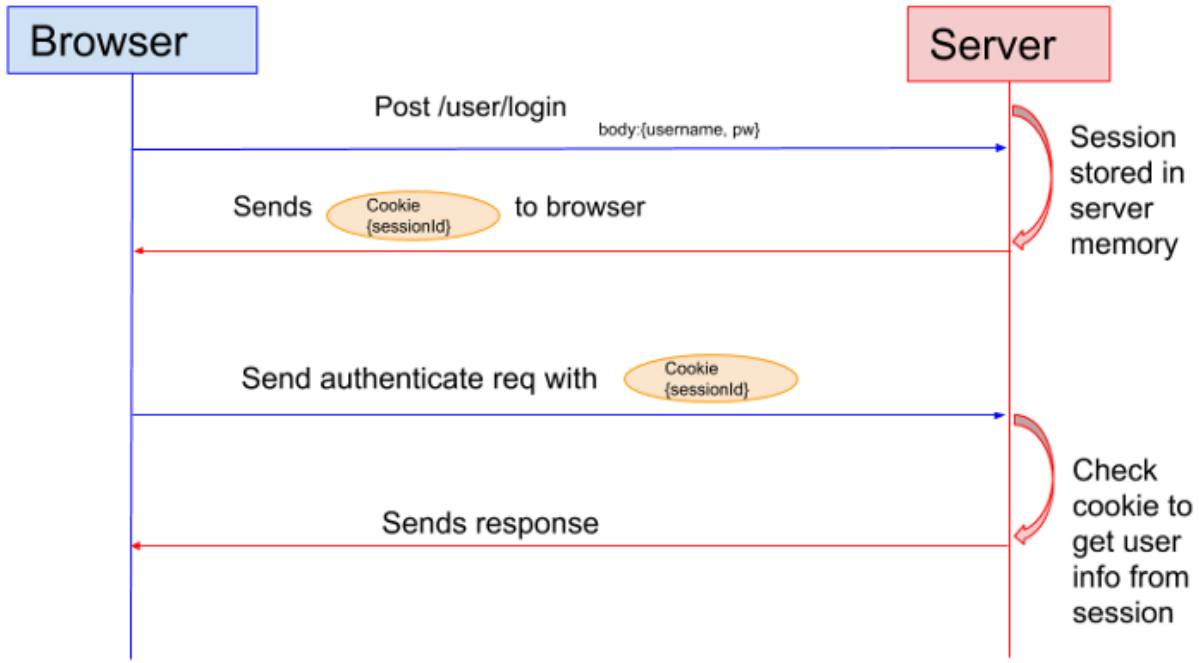
# STRATÉGIE DE SÉCURISATION DE MOT DE PASSE

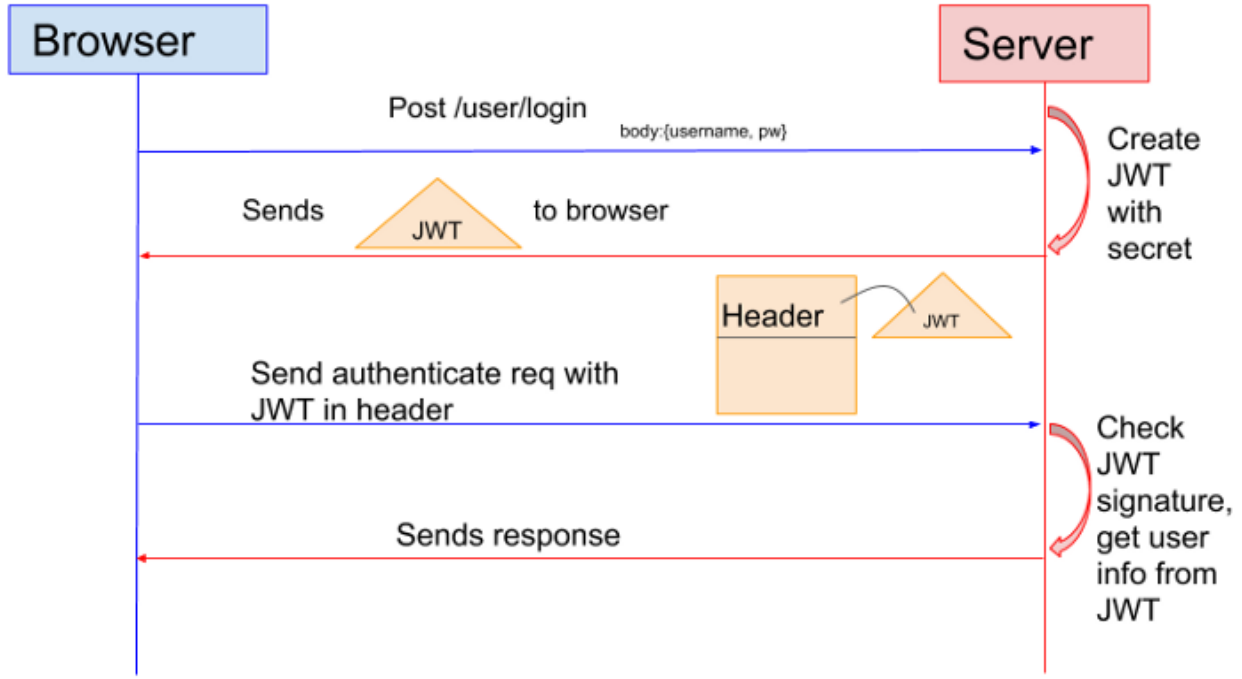


# SALAGE - HASHAGE - ENCODAGE

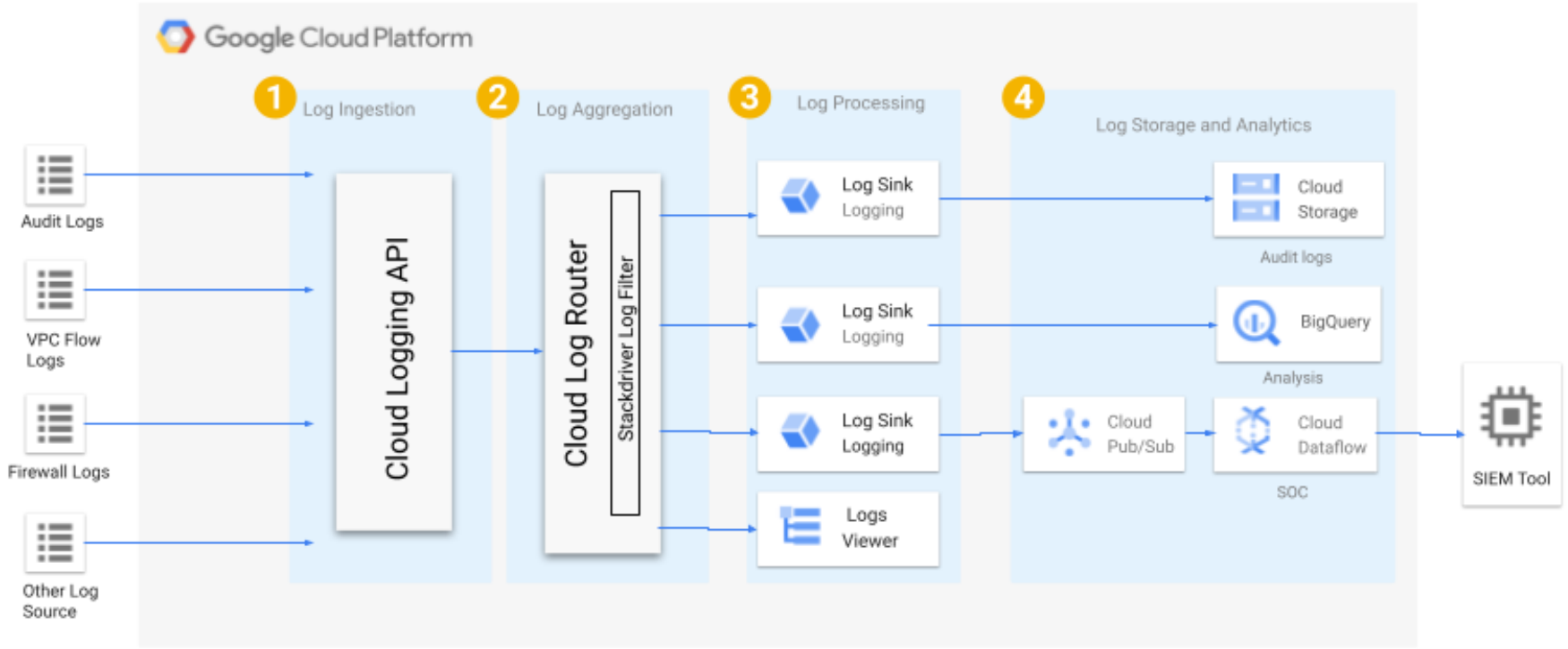


# SESSION - TOKEN



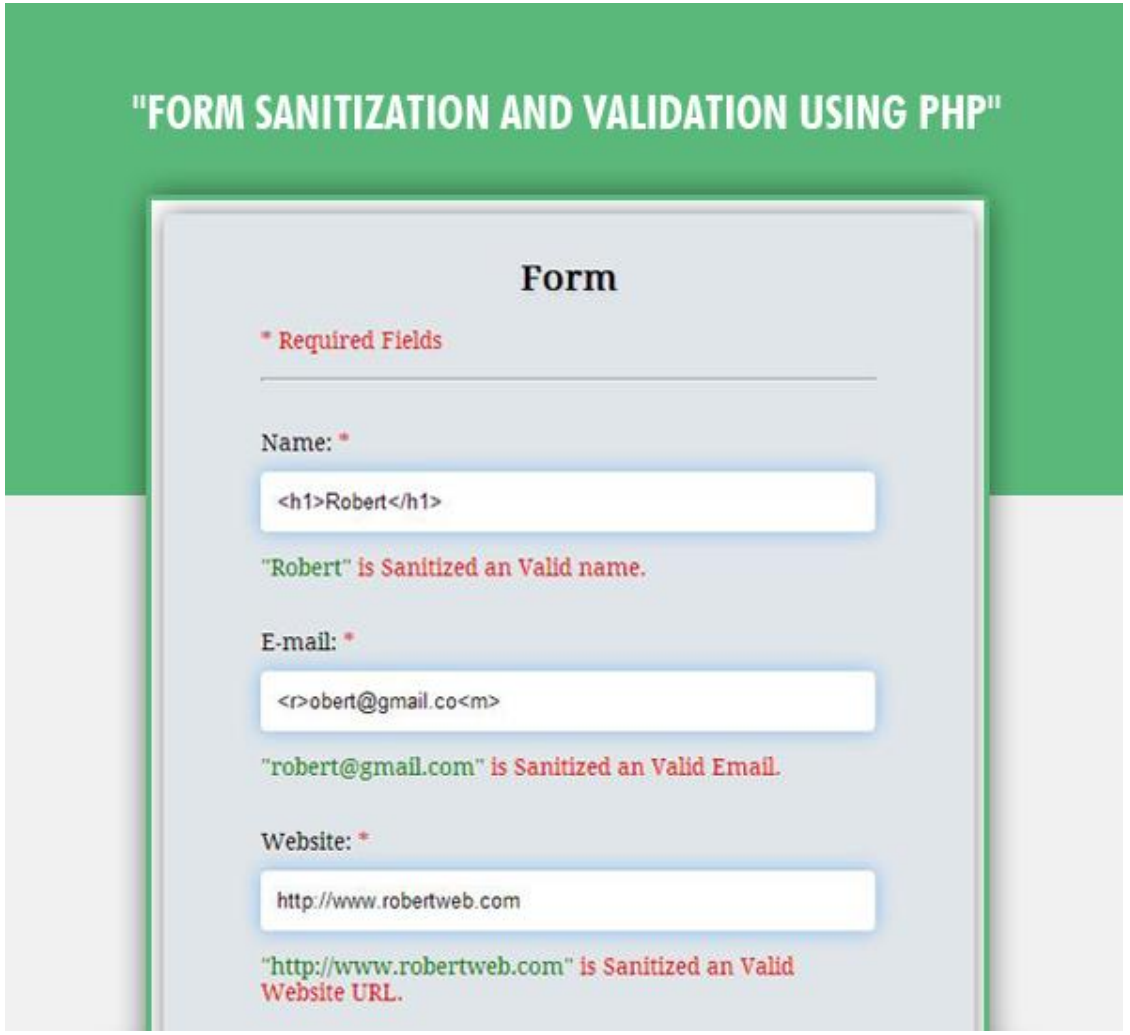



# JOURNALISATION

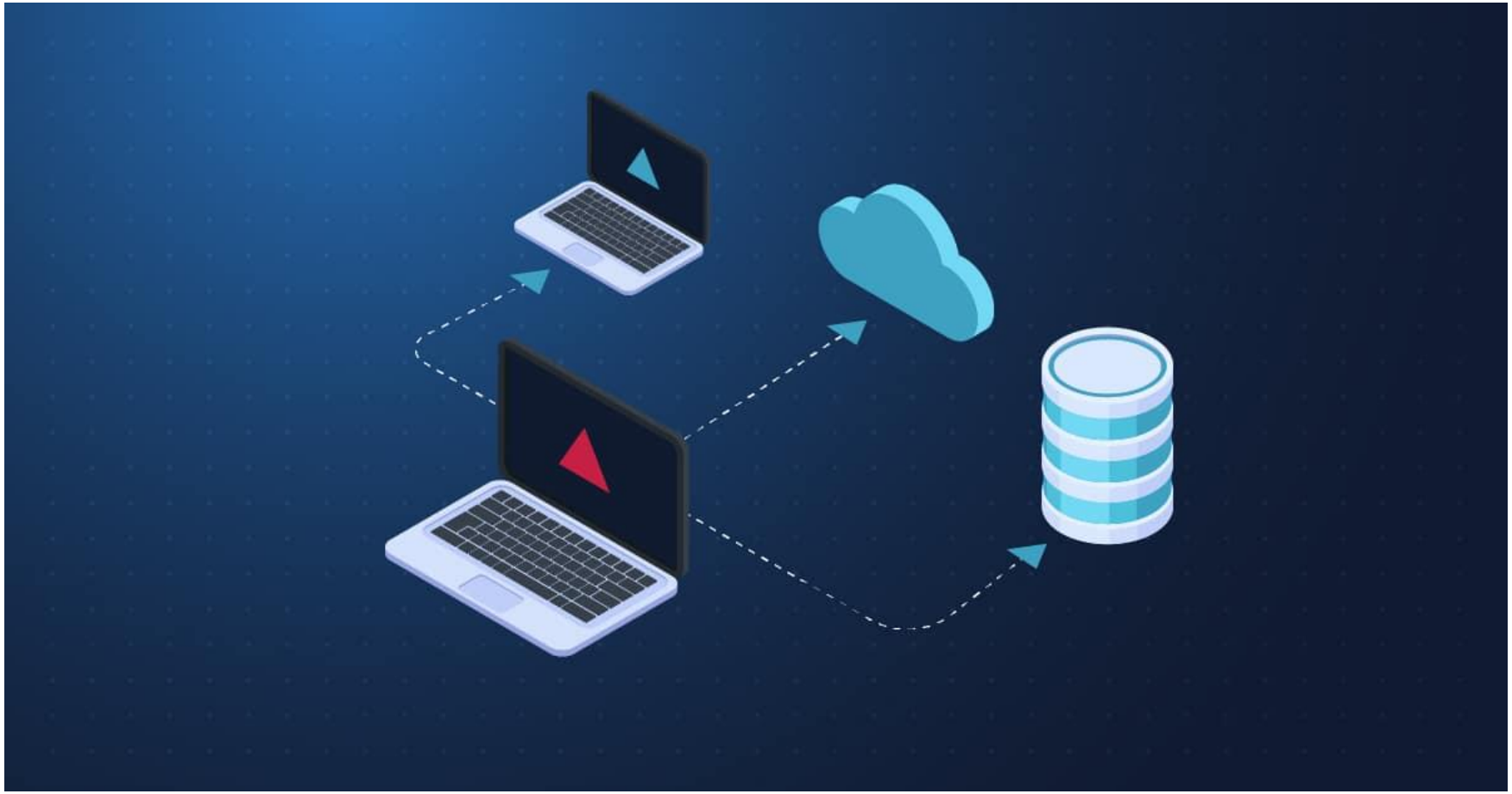



SIEM - Security Information Event Management

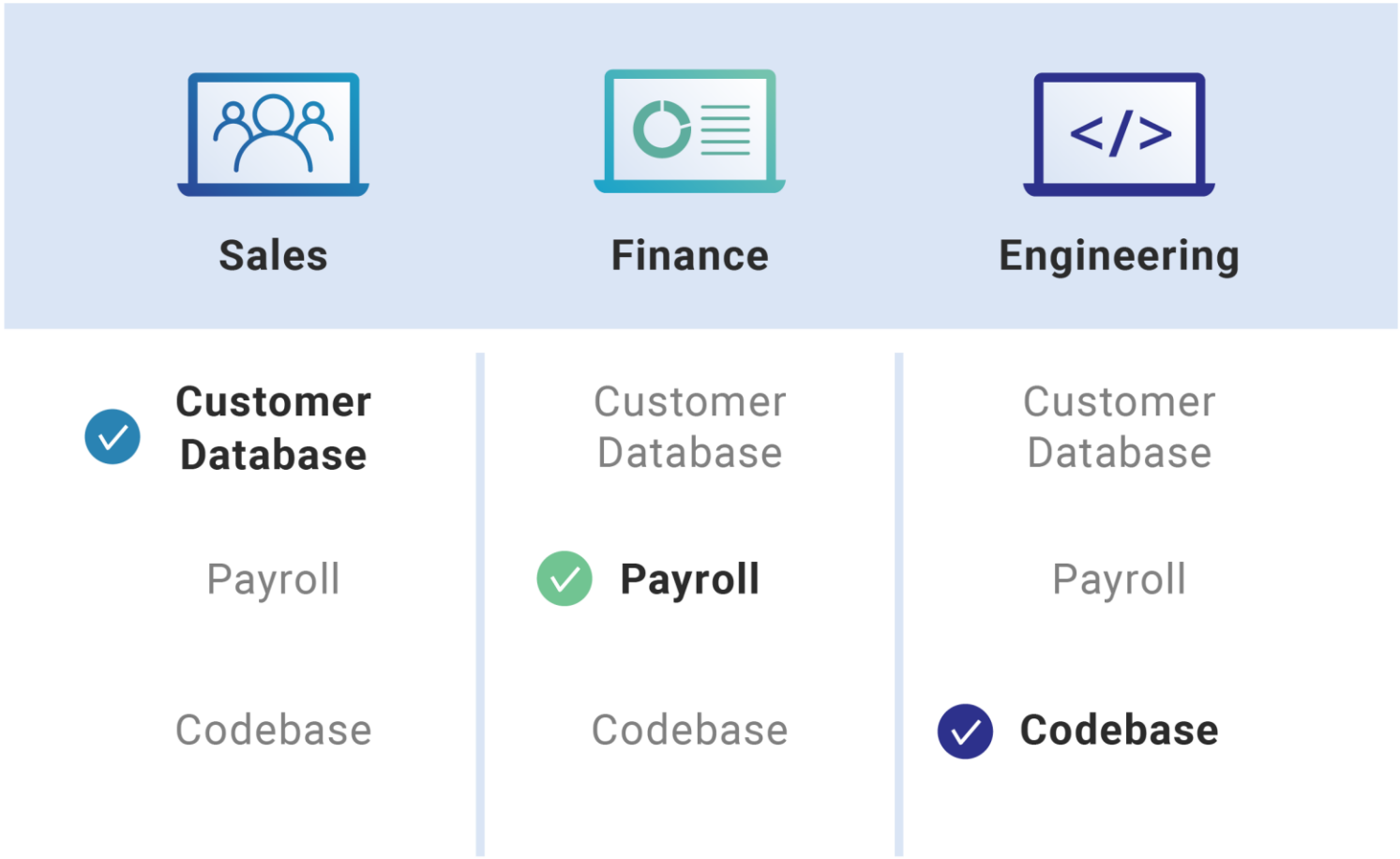
# SANITIZATION



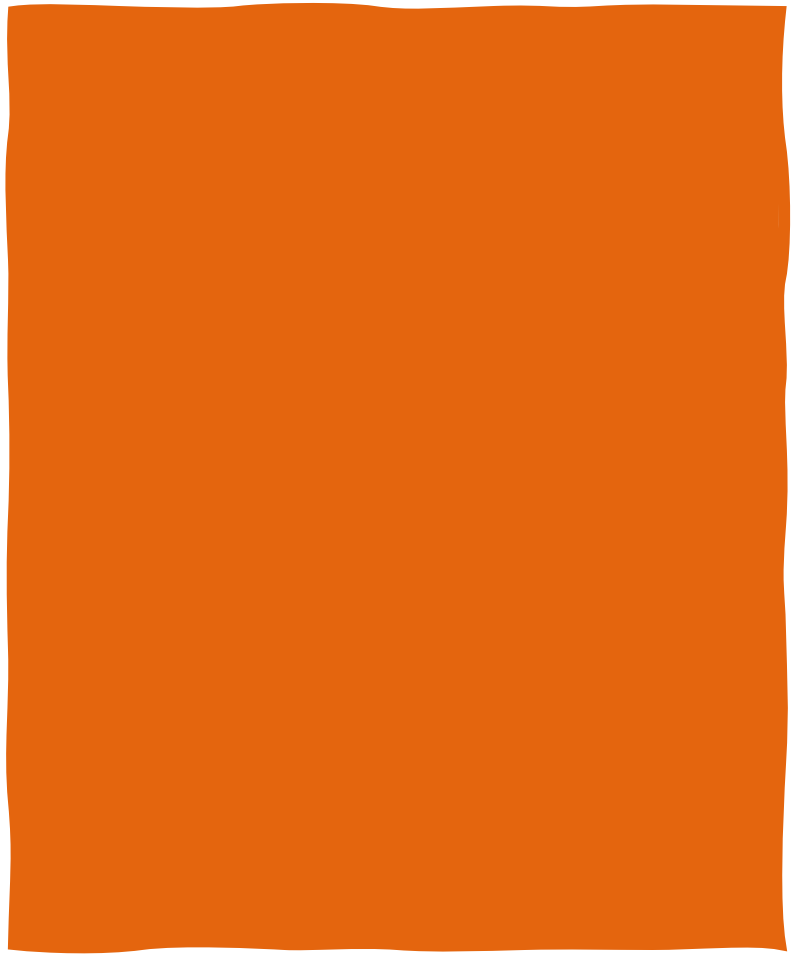
# STRATÉGIE DE SAUVEGARDE



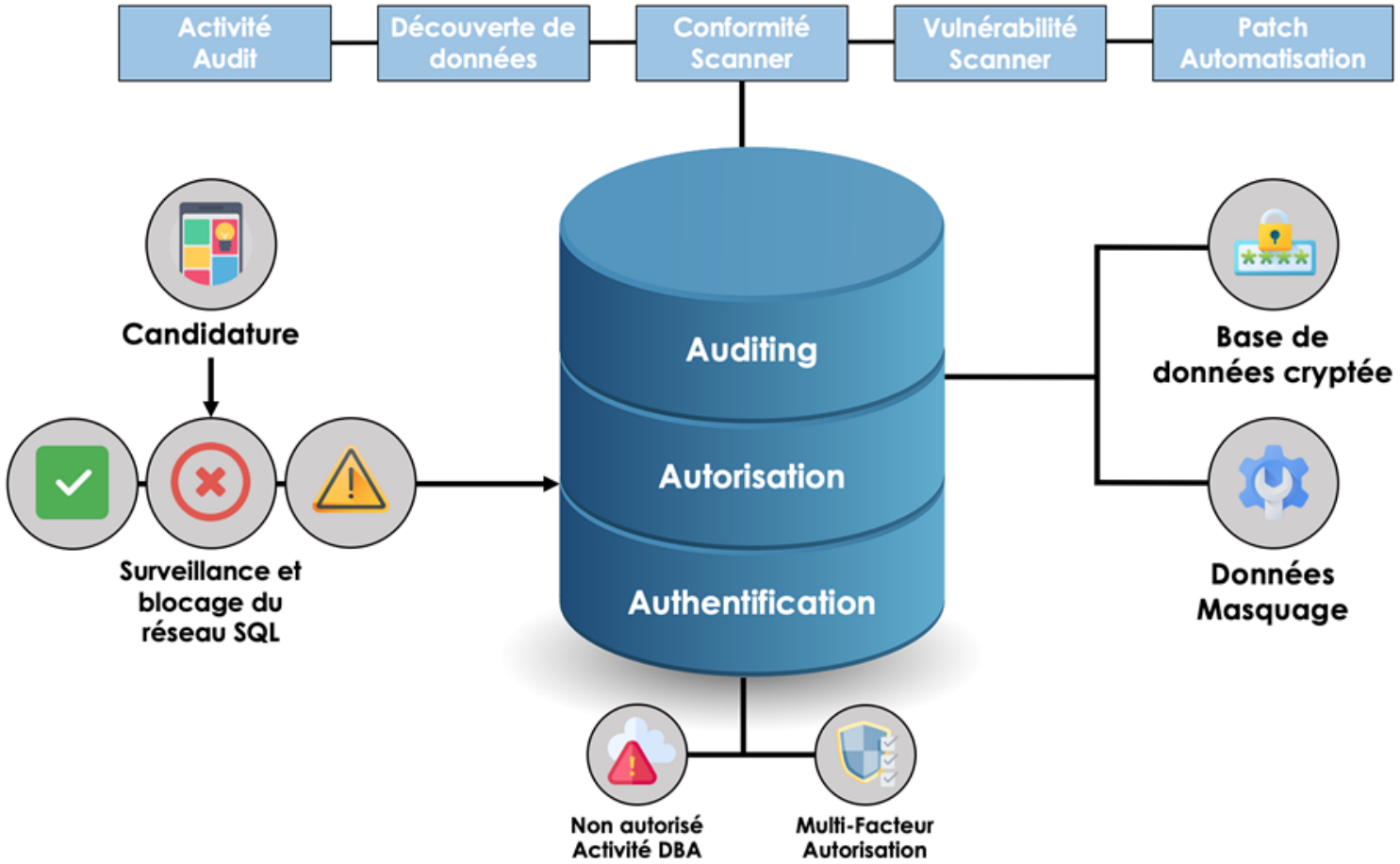
# LE CONTRÔLE D'ACCÈS BASÉ SUR LES RÔLES (RBAC)



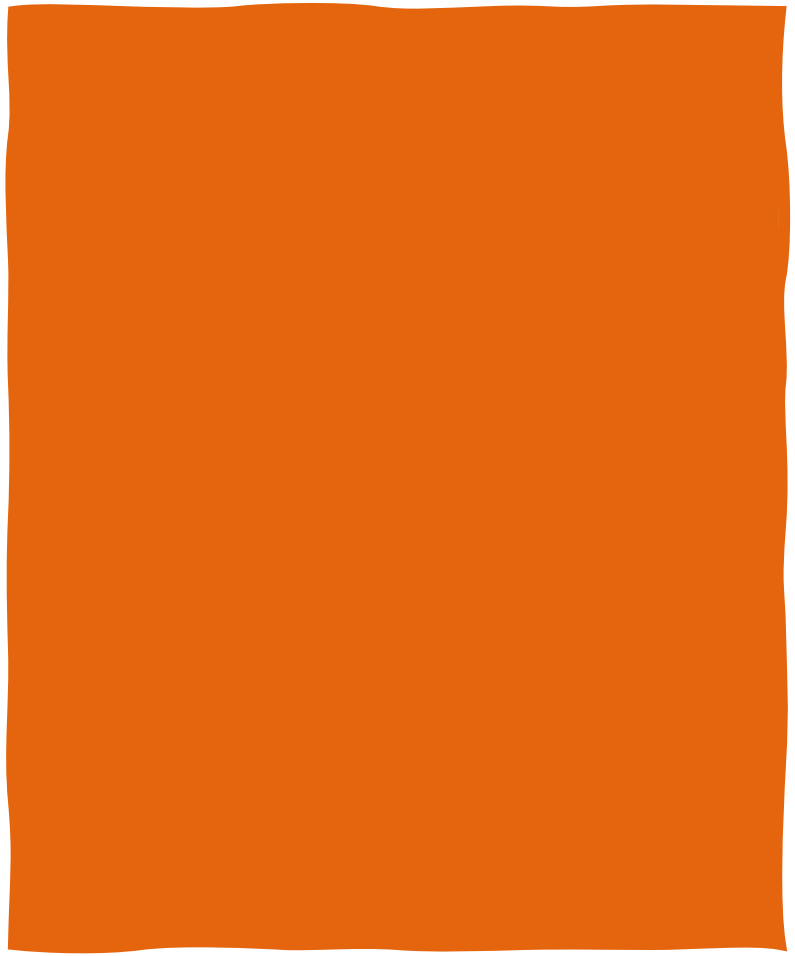
# SÉCURISATION BASE DE DONNÉES



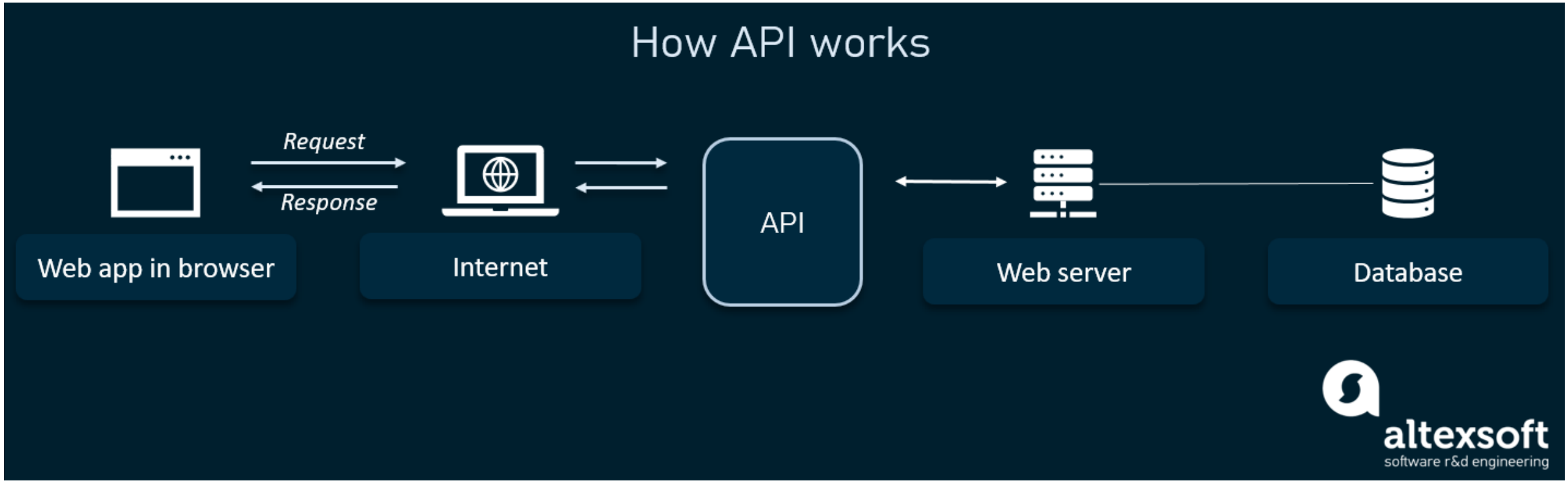
# SÉCURISATION BASE DE DONNÉES



# SÉCURISATION API



# INTERFACES DE PROGRAMMATION D'APPLICATIONS (API)



# FIN