

Offre **Sécurisation des API**

in good we trust.



Sécurisation des Application Programming Interfaces

Contexte

La **généralisation des APIs** est issue de la **transformation du modèle d'exposition et de consommation des applications**, désormais orientées **micro-services**.

Cet engouement pour les API prend sa source dans leurs **capacités d'automatisation** possibles, raison d'être du **Cloud Computing**.

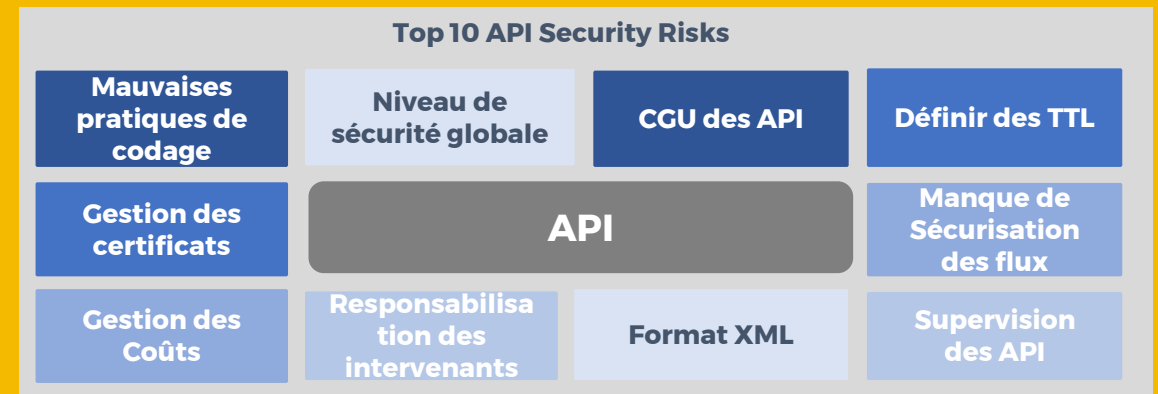
Le développeur doit intégrer dans son codage:

- Bonne pratique de codage
- L'authentification
- Le chiffrement
- Gestion des API



Enjeux

- API, une cible de choix pour les pirates afin d'**accéder à des informations sensibles**.
- Gartner estime que **les fuites de données** via API seront plus fréquentes que celles réalisées via les sites Web d'ici 2022.



good questions.

Qui sont les acteurs ?

Google Apigee
IBM, Ca Technologies
MuleSoft, Red hat, Axway, Moskitos...

API et ma gouvernance

Contrôle d'identité, d'accès
de vulnérabilité
Gestion de risque
Cycle de vie, version



Quels menaces ?

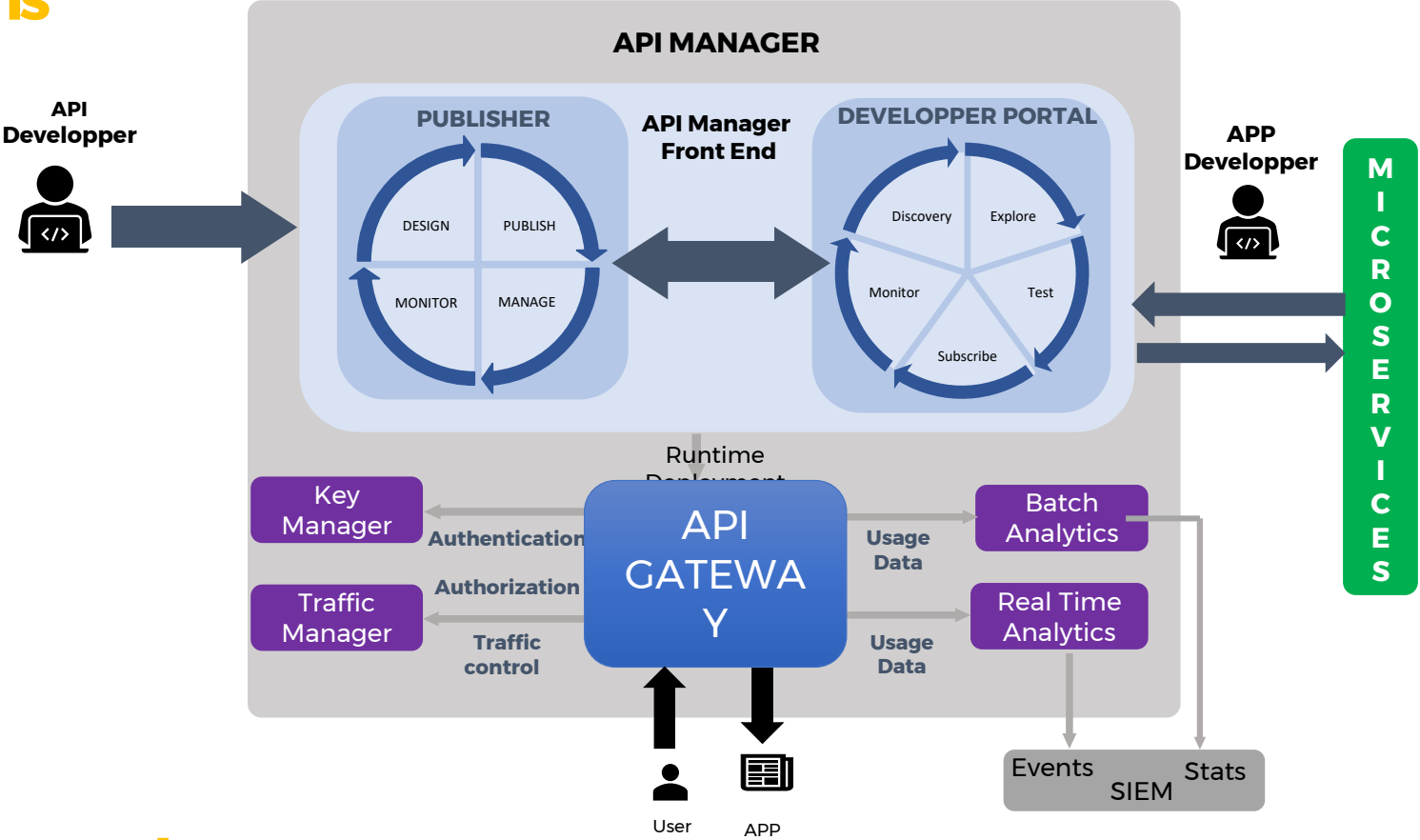
Fuite et intégrité des données
DDOS (Déni de Service)
Injection SQL
MTM (Man in the Middle)

Quelles Solutions ?

OIDC (OpenID Connect)
API manager
WAF(Web Application Firewall)/ API Gateway

Sécurisation des Application Programming Interfaces

good solutions



good practice & tech.

