Vocabulaire DevSecOps - Introduction

- Sécurité intégrée dès le début du cycle : shift-left
- Formation des équipes : attaques, outils, bonnes pratiques

CIA - Confidentialité, Intégrité, Disponibilité

- Confidentiality : accès limité aux autorisés
- Integrity : données non altérées sans autorisation
- Availability : données accessibles quand nécessaire

Le SIEM - Rôle et objectifs

- Agrégation des données
- Corrélation des évènements
- Collecte temps réel

SIEM - Corrélation et archivage

- Profil type de l'infrastructure
- Détection anomalies en temps réel
- Archivage long terme pour conformité

Comparatif solutions SIEM

- Splunk (Commercial, puissant mais cher)
- ELK (Open Source, modulaire, plus complexe)
- IBM QRadar (Commercial, automatisation avancée)
- Wazuh (Open Source, léger pour PME)

Comparatif des solutions SIEM

Solution	Type	Cas d'usage	Avantages	Inconvénients
Splunk	Commercial	Grandes entreprises Conformité réglementaire	Interface intuitive Capacité à scale	Coût très élevé pour des volumes de données importants
ELK	Open source	Environnements agiles Startups	Modulaire Gratuit	Complexité de mise en œuvre
IBM QRadar	Commercial	Grandes entreprises avec de fortes exigences réglementaires	Automatisation plus élaborée	Courbe d'apprentissage élevée
Wazuh	Open source	PME	Léger	Fonctionnalités limitées

Intégration SIEM & DevSecOps avec agents de collecte Fluentd/Filebeat

- Collecte des logs des pipelines CI/CD
- Stratégique pour :
  - détecter les anomalies en temps réel, comme les activités suspectes ou les modifications non autorisées à l'intérieur des pipelines CI/CD ;
  - automatiser les réponses en arrêtant les processus malveillants et en bloquant les IP de manière automatique ;
  - maintenir la conformité de l'infrastructure pour respecter les exigences et régulations comme le RGPD ou le PCI-DSS.

- Fluentd : input, filter, output
- 500+ plugins, intégration SIEM & Cloud

Fluentd

- Fluentd repose sur trois concepts :
  - **Input** : collections des logs provenant de diverses sources (Python, HTTP, Docker, Cisco, etc.) ;
  - **Filter** : transformation des logs et ajouts d'informations ;
  - **Output** : transmission des logs formatés et enrichis à des systèmes cibles (Elasticsearch, Kibana, Datadog, etc.).