Wazuh

LA PLATEFORME DE SÉCURITÉ OPEN SOURCE

Présentation

- SIEM
  - Security information and event management
- XDR
  - Extended Detection and Response
- Licence
  - GNU GPLv2
  - Code source sur Github

Fonctionnement

- Agent
  - Multiplateformes
  - Léger
- Indexer
  - Indexation
  - Recherche
  - OpenSearch

Fonctionnement

- Dashboard
  - Page web
  - Configuration
  - Analyse
- Server
  - Analyser
  - Traiter
  - Association

Fonctionnalités

- Inventaire
  - Matériel
  - Applications
  - Réseau
- Suivi d'intégrité
  - Registre Windows
  - Dossiers / Fichiers
- Scanner de vulnérabilité
- Configuration de sécurité
  - Center for internet security

Fonctionnalités

- Conformité
  - RGPD
    - IV.32.2 : "*Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite*."
  - PCI DSS
  - HIPAA
  - NIST 800-53

Cas d'usage

- Vérification de mise à jour
- Surveillance des évènements de connexions
- Surveillance de l'intégrité de clé SSH