UQAC
Université du Québec
à Chicoutimi

Wazuh

mise en place d'un SIEM

- objectif :
  - Monter une petite architecture avec un conteneur client, un conteneur serveur, et un conteneur « outil de gestion »
  - expérimenter la génération de logs pour alimenter une base de gestion
  - utiliser des jeux de données disponibles sur le site Wazuh pour apprendre à détecter des évènements, à les caractériser et à les catégoriser
- Matériel :
  - une machine virtuelle linux sur votre ordinateur, avec Docker pour créer des conteneurs
  - support : pdf fourni
- Difficulté :
  - moyenne, en fonction de votre niveau en linux