Vous faites partie d'un SOC en tant qu'Analyste redteam, votre Manager vous demande de réaliser l'automatisation d'action que vous réalisez tous les jours afin de vous faire gagner du temps sur vos tâches journalières.

L'objectif du projet se définit dans la recherche et la collecte des informations spécifiques :

Automatisation des actions RED TEAM :

- L'objectif est de réaliser un playbook d'automatisation « toolbox ». Dans un objectif de continuité de vos cours précédents il est nécessaire de nous faire parvenir vos idées par le biais d'idées comme par exemple :
  - Automatisation d'un test d'intrusion (création d'un scan de vulnérabilités)
  - Récupération (scrapping) des vulnérabilités critiques 'up-to-date' dans un objectif purple team afin de contribuer avec l'équipe blue team au suivi du patching de votre société.
  - Recherche OSINT sur un domaine stratégique (google dorks par exemple…) afin d'identifier les menaces
  - Collecte du modèle MITRE ATTCK d'une menace (Tactique, Technique, Mitigation)
  - … il y a énormément d'idées à vous d'être force de proposition !! ☺

RENDU :

Il est demandé aux étudiants de fournir le code source dûment documenté du travail, ainsi qu'un rapport complet sur son utilisation. RENDU le 15 fevrier 2023.