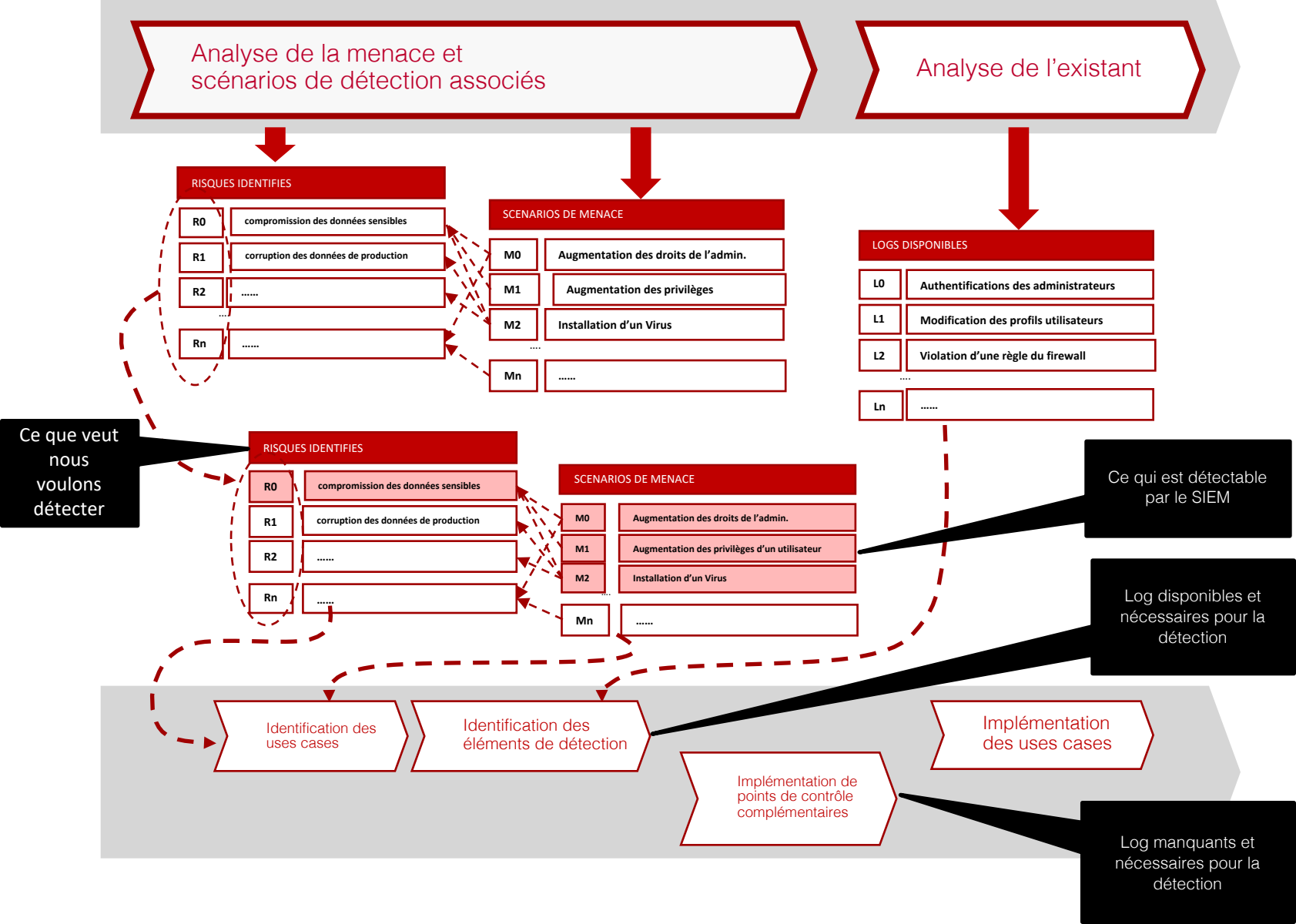
Analyse de la menace et scénarios de détection associés
Analyse de l'existant
RISQUES IDENTIFIES
R0
compromission des données sensibles
R1
corruption des données de production
R2
.....
Rn
.....
SCENARIOS DE MENACE
M0
Augmentation des droits de l'admin.
M1
Augmentation des privilèges
M2
Installation d'un Virus
Mn
.....
LOGS DISPONIBLES
L0
Authentifications des administrateurs
L1
Modification des profils utilisateurs
L2
Violation d'une règle du firewall
Ln
.....
Ce que veut nous voulons détecter
RISQUES IDENTIFIES
R0
compromission des données sensibles
R1
corruption des données de production
R2
.....
Rn
.....
SCENARIOS DE MENACE
M0
Augmentation des droits de l'admin.
M1
Augmentation des privilèges d'un utilisateur
M2
Installation d'un Virus
Mn
.....
Ce qui est détectable par le SIEM
Log disponibles et nécessaires pour la détection
Identification des uses cases
Identification des éléments de détection
Implémentation des uses cases
Implémentation de points de contrôle complémentaires
Log manquants et nécessaires pour la détection