|  |
| --- |
| MIMIR |
| Massive Information Management for Incident Response |

|  |
| --- |
| BUEE Olivier – 2nd semestre 2021  Projet mené dans le cadre de l’unité d’enseignement UTC 504 du CNAM |

Table des matières

[1. Préambule 2](#_Toc66136347)

[2. Expression et définition des besoins 2](#_Toc66136348)

[2.1 Expression du besoin (Interview) 2](#_Toc66136349)

[2.2 Définition du besoin (Cahier des charges) 2](#_Toc66136350)

[3. MERISE 2](#_Toc66136351)

[3.1 Analyse du cahier des charges 2](#_Toc66136352)

[3.2 Modèle conceptuel de données 2](#_Toc66136353)

[3.3 Modèle logique de données 2](#_Toc66136354)

[3.4 Modèle relationnel 2](#_Toc66136355)

[3.5 Création de tables SQL 2](#_Toc66136356)

[4. UML 2](#_Toc66136357)

[5. Requêtes SQL 2](#_Toc66136358)

[6. Implémentation technique 2](#_Toc66136359)

# 1. Préambule

Ce projet est développé dans le cadre de l’unité d’enseignement (UE) UTC 504 « Systèmes d’Information et bases de données ». L’objectif de ce projet est de concevoir et réaliser une base de données en utilisant des outils et méthodes dédiées à la conception orientée objet (UML : *Unified Modeling Language)* et au développement de logiciels (MERISE).

# 2. Définition du besoin

## Cadrage

Un centre de réponse à incident (CERT : Computer Emergency Response Team) a pour objectif de déployer des équipes dans des organismes touchés par une attaque informatique.

L’objectif de ces équipes est alors de contenir les attaquants en détectant les traces laissées par ces derniers.

Pour ce faire, ces équipes ont besoin de s’appuyer sur un outil pour capitaliser/partager/résumer les éléments techniques pertinents, ainsi que le résultat de leurs investigations.

Cet outil doit permettre à minima de :

* créer des artefacts systèmes et/ou réseaux ;
* lier ces marquants à un attaquant pour le caractériser et définir son mode opératoire.

L’outil doit également permettre de créer des objets permettant de capitaliser les connaissances sur le contexte de l’entreprise, notamment sur :

* le système d’information (SI) ;
* les biens essentiels et les systèmes critiques ;
* ses utilisateurs.

Enfin l’outil doit permettre de lier tous ses éléments pour éditer un suivi chronologique des analyses et actions effectuées par les analystes, mais également sur le mode opératoire de l’attaquant.

## Déroulement du projet

Le projet s’appuiera sur une gestion de projet dite agile (type Scrum).

Cette approche incrémentale permettra de fournir rapidement des premiers éléments exploitable, suivi d’un premier livrable avec les fonctions essentielles du projet. Cette méthode de développement permettra ainsi d’adapter les attendus du livrable final en se basant sur des retours d’expérience, mais également d’évoluer au travers d’une méthode empirique.

Les fonctions essentielles attendues correspondent aux attendus définis sur la ligne « réussite acceptable » de la matrice des objectifs présentée ci-dessous.

|  |  |  |
| --- | --- | --- |
|  | **Livrable** | **Documentation** |
| **Insuffisant** |  |  |
| **Réussite acceptable** | Création de marquant technique système et/ou réseau.  Création de *Endpoint*.  Liaison entre marquant technique et *Endpoint*. | Explication minime introduite directement au sein de l’application |
| **OK** | Lier les marquants techniques à un acteur malveillant  Contextualiser les Endpoint grâce à la liaison avec des utilisateurs et des zones logiques (LAN) et zones géographiques (site, bâtiment, pièce) | Documentation utilisateur complète |
| **Excellent** | Ajout de fonctionnalités tel que la liste des TTPs selon la matrice Mitre Att&ck. Import d’une liste d’utilisateur et machine  Export d’élément technique vers une application tierce. | Documentation administrateur |

Figure 1 : Matrice des objectifs

Afin de concentrer les efforts sur le fonctionnement interne du projet, le projet s’appuiera sur un framework Web type Django, afin de faire abstraction de l’aspect gestion de compte utilisateur, sécurité de l’application, … .

# 3. MERISE

## 3.1 Analyse du cahier des charges

L’analyse des besoins exprimés a permis de définir le tableau suivant :

|  |  |  |
| --- | --- | --- |
| **Entité** | **Attributs** | **Commentaire** |
| Artifact | Artifact\_ID  Artifact\_Name  Artifact\_Type  Artifact\_Status  Artifact\_TTP  Artifact\_Comment | Cette entité permettra de capitaliser les informations trouvées à la suite d’investigation. |
| Endpoint | Endpoint\_ID  Endpoint\_Name  Endpoint\_Type  Endpoint\_Status  Endpoint\_Function  Endpoint\_Criticality  Endpoint\_Comment | Cette entité regroupera les informations connues concernant un équipement. |
| Utilisateur | User\_Account  User\_Name  User\_Surname  User\_Status  User\_Function  User\_Criticality  User\_Comment | Cette entité regroupera les informations connues sur un utilisateur. |
| Zones / LAN | Area\_Name  Area\_Criticality  Area\_Comment | Cette entité permettra de situer les *Endpoint* et utilisateurs et ainsi évaluer l’évolution de la menace. |
| Attaquant | Actor\_Name  Actor\_Type  Actor\_Aim  Actor\_TTPs  Actor\_Comment | Cette entité permettra de caractériser la menace. |

L’élément principal de l’outil se base sur les éléments « Marquant technique » et « *Endpoint »*. Le travail effectué par les analystes de la réponse à incident viendra compléter les attributs de ces éléments.

Ces deux éléments seront liés par une association (« Corrupt »), les attributs contenus dans cette association pourront permettre de faire un suivi chronologique des événements.

Les autres entités (« Attaquant », « User » et « Zone ») permettent d’ajouter du contexte et ainsi faciliter la priorisation des actions.

Contrainte d’intégrité :

La date de fin de compromission devra toujours être supérieure à la date de début de compromission.

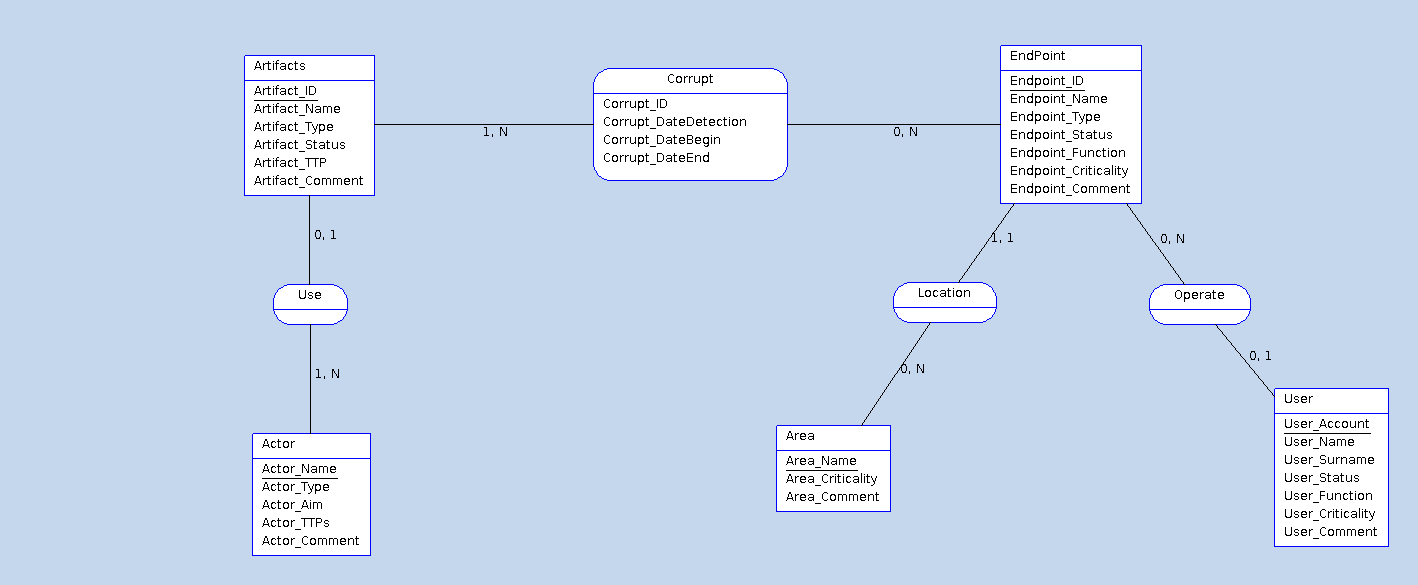
Evolution envisageable :

* Permettre de suivre les évolutions (historique) d’un marquant technique.

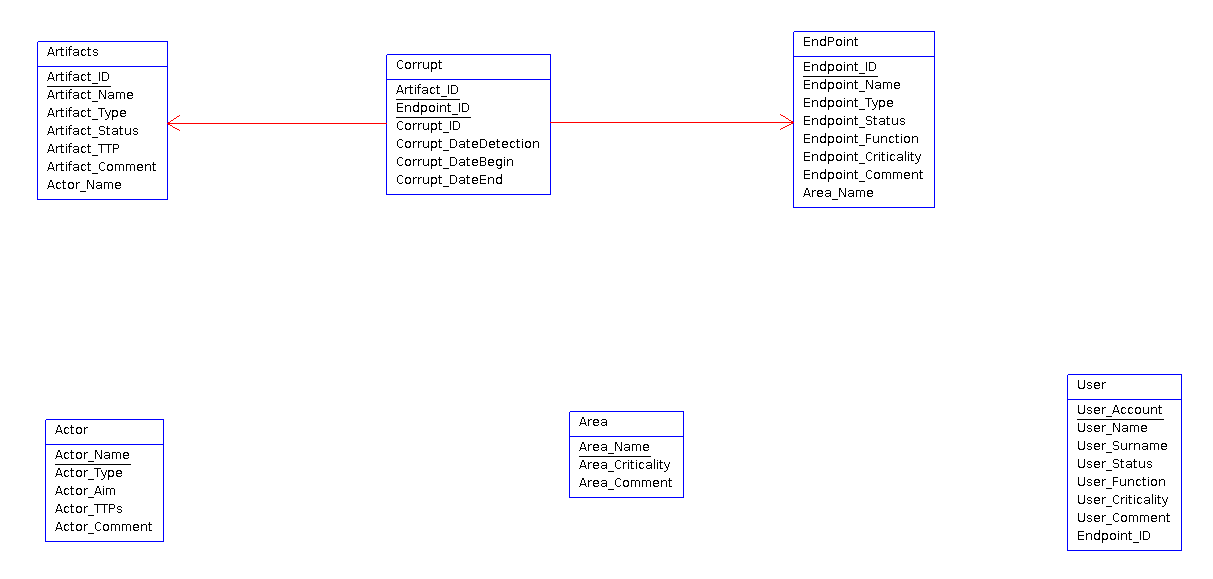
*Exemple dans le cas d’une compromission type « supply chain », une communication vers un partenaire de confiance doit pouvoir passer de l’état légitime à malveillant, tout en gardant l’historique des qualifications passées. (Ajout d’un ID au marquant technique pour gérer l’historique)*

- Intégrer les Tactiques, Techniques et Procédures (TTP) défini dans la matrice Mitre Att&ck dans une table pour s’appuyer sur une base existante.

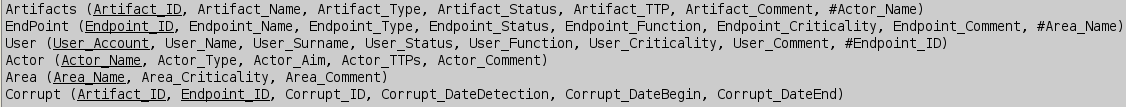
## 3.2 Modèle conceptuel de données

**

## 3.3 Modèle logique de données



## 3.4 Modèle relationnel



## 3.5 Création de tables SQL

# 4. UML

# 5. Requêtes SQL

# 6. Implémentation technique