Sécurisation d'un réseau informatique dédié à la vidéoprotection

Julien Trelat

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

CENTRE REGIONAL ASSOCIE D'AUVERGNE – RHÔNE-ALPES

Mémoire présenté en vue d'obtenir

LE DIPLOME D'INGENIEUR CNAM

Spécialité : INFORMATIQUE parcours Systèmes d'Information

par

Julien TRELAT

Sécurisation d'un réseau informatique dédié à la vidéoprotection

Soutenu le 29 juin 2021

JURY

PRESIDENT :	**Christophe PICOULEAU**	***Enseignant au CNAM***
MEMBRES :	**Ekaterina BOUROVA**	***Enseignante au CNAM et Tutrice Pédagogique***
	Gérald MOREL	***Ingénieur Informatique CARSAT***
	Lilian RAYNAUD	***Directeur Technique Securitas et Tuteur d'Entreprise***

Remerciements

Je tiens tout d'abord à exprimer toute ma gratitude à mon épouse Garance ainsi que mes enfants Léo et Louise qui m'encouragent continuellement et qui font preuve d'une grande compréhension face à mes périodes d'isolement nécessaires depuis la rentrée 2016 afin de préparer ce diplôme.

Mes remerciements se tournent également vers l'ancien directeur général de l'entreprise Gilles BONNEFOY qui a été très enthousiaste face à ma démarche de reprise de mes études et qui m'a toujours poussé et donné les moyens pour aller au bout. Merci également à son remplaçant Laurent ZAFFRAN qui continu dans sa lancé en me faisant confiance et en continuant de m'encourager.

Je remercie aussi mon ancien responsable Laurent POMMIER qui m'a permis d'étudier ce sujet dans le cadre de ce mémoire ainsi que mon responsable actuel et directeur technique de l'entreprise Lilian RAYNAUD qui me prodigue de précieux conseils au quotidien dans l'exercice de mes fonctions.

Enfin, je remercie tous les enseignants du CNAM qui ont su donner de l'intérêt dans leurs enseignements et qui m'ont donné l'envie d'apprendre et de poursuivre ce cursus jusqu'à la fin.

Table des matières

Table des figures

Table des tableaux

Glossaire

Mot :	Définition :
Analyse de risque :	Ensemble de processus permettant l'identification, l'évaluation et le traitement des risques pesant sur un système d'information
Authentification :	Procédure visant à contrôler l'identité d'une personne ou d'un équipement informatique
Cloisonnement :	Dans un réseau local, le cloisonnement consiste à diviser le réseau en plusieurs sous-réseaux pour des raisons de fonctionnement ou de sécurité
Contrôle d'accès :	Moyens techniques mis en œuvre pour gérer et sécuriser les accès à un système d'information ou un réseau local
Cybersécurité :	Ensemble de moyens techniques ou organisationnels mis en œuvre pour assurer la sécurité d'un système d'information et notamment des données qu'il traite
Imputabilité :	Fait d'attribuer une action (accès à un système d'information, à une donnée) à une personne ou ressource
Mesure de sécurité :	Moyen technique ou organisationnel permettant de traiter un risque
Non-répudiation :	Fait de ne pouvoir nier ou rejeter qu'un événement (accès à un système d'information, à une donnée) a eu lieu
Réseau local (LAN) :	Réseau informatique composé des équipements et liaisons nécessaires à la communication des éléments qui le compose
Réseau local virtuel (VLAN) :	Réseau informatique logique appartenant à un réseau local. Plusieurs réseaux locaux virtuels peuvent cohabiter au sein du même réseau local
Vidéoprotection	Installation composé de caméras et de systèmes de transmission, de stockage et de visualisation des images permettant la surveillance d'un espace à distance

Abréviations

AAA : Authentication Authorization Accounting

AC : Autorité de Certification

AE : Action Elémentaire

ANSSI : Agence Nationale de la Sécurité des Système d'Information

CERT : Computer Emergency Response Team

CID : Confidentialité Intégrité Disponibilité

CNPP : Centre National de la Prévention et de la Protection

EAP : Extensible Authentification Protocol

EBIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ER : Evénement Redouté

IGC : Infrastructure de Gestion des Clés

NAS : Network Access Server

OV : Objectif Visé

PACS : Plan d'Amélioration Continue de la Sécurité

RADIUS : Remote Authentication Dial-In User Service

SGDSN : Secrétaire Général de la Défense et de la Sécurité Nationale

SI : Système d'Information

SR : Source de Risque

TLS : Transport Layer Security

VLAN : Virtual Local Area Network

VMS : Video Management Software

Introduction

La sécurité des systèmes d'information, de nos jours nommée « Cybersécurité », est un sujet très en vogue actuellement. Les attaques informatiques sont monnaie courante, pas un jour ne passe sans qu'une actualité ne relaie le cas d'une organisation victime d'une cyberattaque ou l'identification de nouvelles menaces cyber.

Depuis sa création en 2009, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), service rattaché au Secrétaire Général de la Défense et de la Sécurité Nationale (SGDSN), ne cesse d'évaluer cette menace et de publier des guides et des recommandations afin de sécuriser les systèmes d'information mis en œuvre par les administrations publiques mais également les entreprises privées ou les particuliers.

Securitas Sécurité Electronique, entreprise proposant l'installation et la maintenance de systèmes de sécurité électronique, possède une partie de ses clients dans un secteur d'activité dit « sensible », regroupant les organisations publiques ou privées jugées stratégiques par l'état.

Autrefois basé sur des composants essentiellement analogiques, ces systèmes de sécurité représentent aujourd'hui des systèmes d'information à part entière qu'il est donc nécessaire de sécuriser, notamment les systèmes de vidéoprotection qui sont composés d'un grand nombre de périphériques réseaux. La sécurisation du réseau du système de vidéoprotection est le sujet de cette étude.

Dans la première partie de ce mémoire, une présentation du projet sera faite, composée de la présentation de l'entreprise Securitas Sécurité Electronique et d'une description du contexte et des objectifs du projet.

Ensuite, la seconde partie consistera à l'analyse de risque d'un système d'information dédié à la vidéoprotection, réalisée par la méthode EBIOS Risk Manager de l'ANSSI.

La troisième partie détaillera quant à elle la solution technique mise en œuvre pour la sécurisation du réseau informatique dédié au système de vidéoprotection en fonction des éléments mis en évidences dans l'analyse de risque, notamment par l'étude et le test de deux mesures de sécurité spécifiques que sont le cloisonnement du réseau et le contrôle d'accès réseau.

Enfin, la quatrième et dernière partie évaluera le coût d'intégration de cette solution technique dans les projets de sécurisation de Securitas Sécurité Electronique et en décrira les prérequis techniques et les méthodes élaborées.

1. Présentation du projet

1.1. Présentation de l'entreprise

Securitas Sécurité Electronique est une entreprise, filiale de l'entreprise Securitas France elle-même membre du groupe international Securitas AB. Composée de 330 collaborateurs, ses activités principales sont l'étude, l'installation et la maintenance de systèmes de sécurité électronique tels que des systèmes de vidéoprotection, de contrôle d'accès, d'alarme anti-intrusion et de détection incendie. L'entreprise est présente sur tout le territoire national au travers de ses 23 agences locales. Elle réalisa sur l'année 2020 un chiffre d'affaire d'environ 49 millions d'euros.

Les secteurs d'activité de l'entreprise sont multiples et variés, du secteur de la santé à celui de la défense en passant par le secteur logistique, bancaire, les collectivités, la distribution ainsi que de nombreuses PME/PMI. Elle travaille exclusivement pour une clientèle de professionnels.

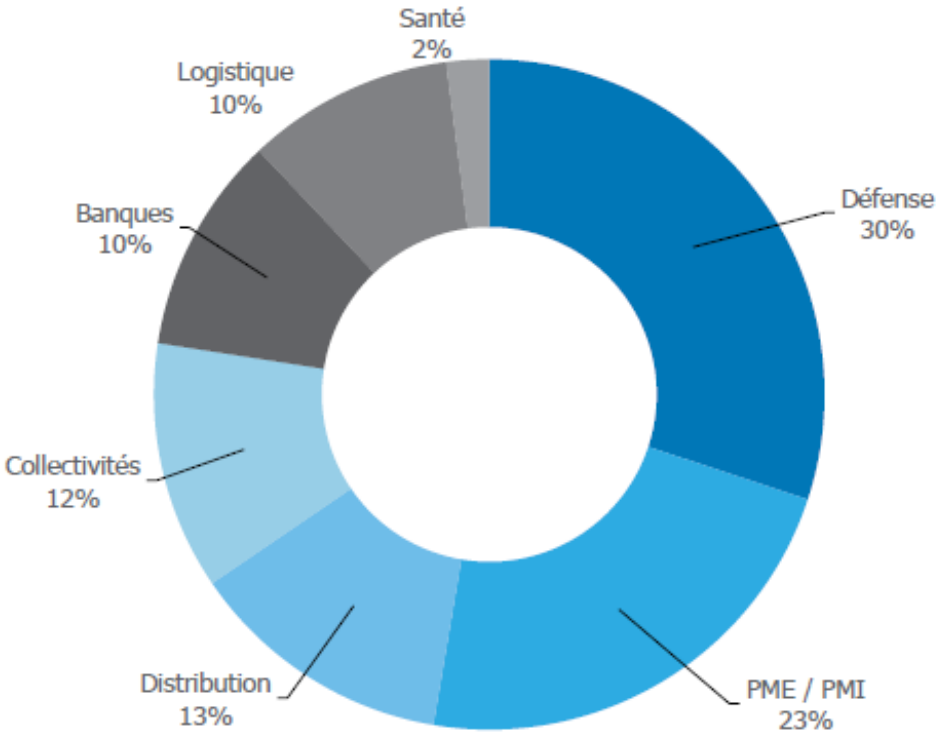

Figure 1 : Répartition de la prise de commande de l'entreprise par secteur d'activité pour l'année 2020

Au sens organisationnel, l'entreprise, dirigée par sa Direction Générale, est divisée en quatre directions supports :

- Direction des Ventes & Alliances
- Direction des Ressources Humaines & Qualité
- Direction Administrative et Financière
- Direction Technique

Elle est ensuite répartie, pour son service opérationnel, en cinq directions régionales et une direction grands comptes qui ont la charge de la réalisation des projets de nos clients.

En tant que Chef de Projets Technique, je fais partie de la Direction Technique qui a en charge plusieurs missions :

- Qualification technique de produits détectés par la Direction des Ventes & Alliances
- Assistance des ingénieurs commerciaux en avant-vente
- Suivi et assistance au suivi de projets complexes pour les clients grands comptes
- Support technique aux agences

Pour réaliser ces missions, la Direction Technique est composée de plusieurs experts techniques aux spécialités différentes (systèmes de contrôle d'accès, de vidéoprotection, administrateur réseau, sécurité informatique…). Le responsable de ce service est le Directeur Technique de l'entreprise.

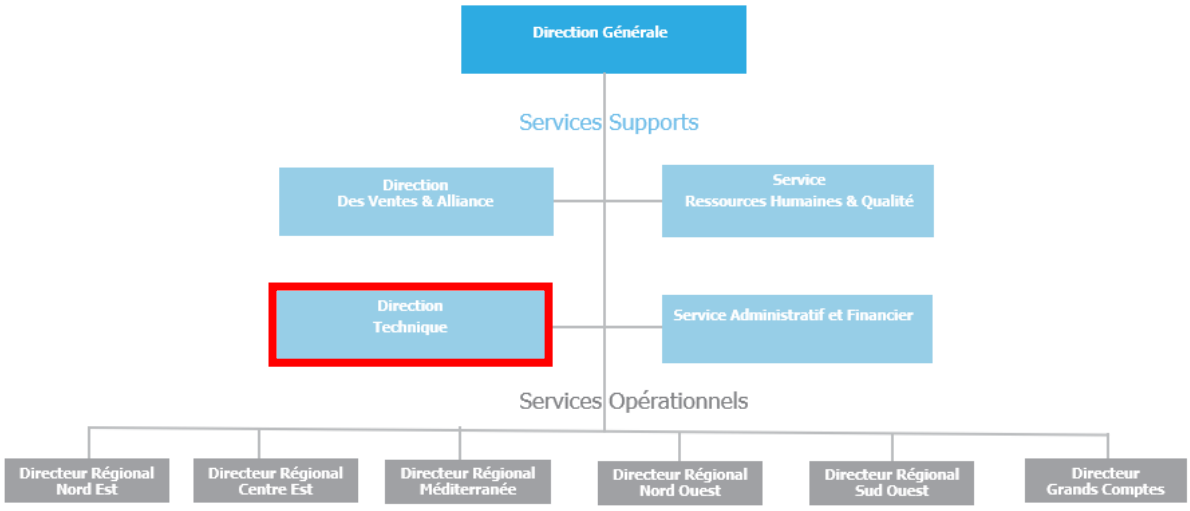

Figure 2 : Organigramme de l'entreprise

1.2. Contexte et objectifs du projet

1.2.1. Des systèmes de sécurité analogiques

La sécurité physique d'un site est assurée par différents systèmes de sécurité électroniques comme les systèmes de détection incendie, d'intrusion ou les systèmes de vidéoprotection. Cette étude porte spécifiquement sur les systèmes de vidéoprotection.

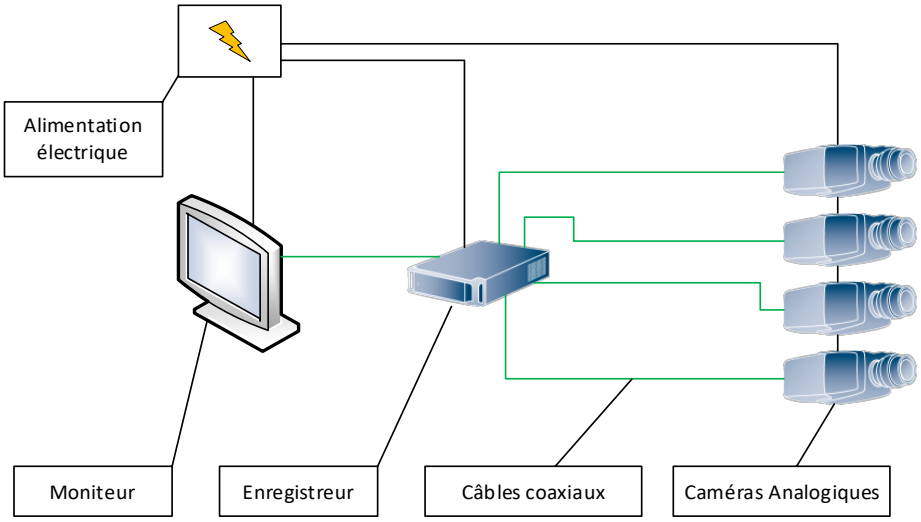

Figure 3 : Système de vidéoprotection analogique

La figure 3 ci-dessus illustre les différents composants nécessaires à un système de vidéoprotection analogique tels qu'ils étaient composés avant la démocratisation des systèmes numériques. Les caméras analogiques étaient directement raccordées à un enregistreur (analogique ou numérique) via des câbles coaxiaux. Un moniteur, également raccordé sur l'enregistreur via un câble coaxial, permettait de visualiser les images en direct ou les enregistrements, le pilotage du système s'effectuant via les boutons disponibles sur l'enregistreur ou une télécommande. Enfin, tous les composants devaient être alimentés électriquement.

Historiquement, ces systèmes étaient mis en œuvre par des entreprises issues de l'électronique ou de l'électricité générale, peu sensibilisées aux normes de la sécurité informatique.

1.2.2. Aux systèmes numériques

Les systèmes analogiques ont peu à peu évolué vers des systèmes numériques, s'appuyant sur des réseaux informatiques, s'identifiant aujourd'hui à des systèmes d'information à part entière.

Pour être fonctionnel, un système de vidéoprotection doit être composé à minima de :

- **Caméras IP** : dispositifs de prises de vues, considérés comme des équipements informatiques, embarquant un ou plusieurs logiciels internes, configurables généralement via une interface web
- **Serveur de gestion** : serveur informatique sur lequel est installé le VMS et équipé de disques durs pour le stockage des images enregistrées. L'utilisation de plusieurs serveurs de gestion est courante dans les systèmes de tailles importantes (plusieurs centaines de caméras IP)
- **Logiciel de gestion vidéo** : appelé VMS (Video Management Software), logiciel ayant la charge de se connecter aux caméras IP afin d'en récupérer les images en direct, puis de stocker ces images sur les disques durs des serveurs de gestion. Il gère également les connexions et droits d'utilisation des postes de visualisation
- **Poste de visualisation** : poste informatique sur lequel est installé un logiciel client du VMS, permettant de visualiser les images en direct et réaliser des relectures et des extractions des images enregistrées. Il existe souvent plusieurs postes de visualisation
- **Commutateur réseau** : équipement servant de nœud de raccordement aux différentes liaisons réseaux et permettant ainsi de créer le réseau informatique connectant entre eux les différents composant du système d'information
- **Liaisons réseaux** : liaisons de différentes natures (filaires, optiques) assurant le transport des informations entre les différents composants du système.

1.2.3. Objectifs du projet

Une partie significative des clients de l'entreprise est soumise à des obligations particulières, notamment ceux faisant partie du secteur d'activité de la défense.

D'une part, l'article L1332-1 du code de la défense stipule que ces organisations sont dans l'obligation d'assurer la protection physique de leurs établissements. Ils doivent donc procéder ou faire procéder à l'installation des systèmes de sécurités adaptés.

D’autre part, les articles L1332-6-1 et L1332-6-3 du code de la défense précisent que les systèmes d’informations mis en œuvre par ces opérateurs doivent être soumis à des mesures de sécurité informatique, et que les contrôles qui peuvent y être menés sur la bonne mise en place de ces mesures seront effectués par l’ANSSI.

Ils doivent donc mettre en œuvre des systèmes d’information répondant aux préconisations de l’ANSSI ou d’autres textes réglementaires en termes de sécurité informatique, or le déploiement des systèmes sécurité en général, de vidéoprotection en particulier sont encore peu souvent contraints à l’application de ces mesures.

L’objectif du projet est donc, en s’appuyant sur les recommandations de l’ANSSI et les différents textes règlementaires, d’établir une solution technique s’appliquant à un système de vidéoprotection déployé sur un réseau informatique et répondant aux exigences de sécurités préconisées ou à l’état de l’art actuel. Cette solution sera considérée par l’entreprise comme une couche « cybersécurité » applicable aux systèmes de vidéoprotection qu’elle installe en général et qu’elle pourra ensuite proposer à ses clients.

Pour atteindre cet objectif, il sera nécessaire de passer par les phases suivantes :

- Réalisation d’une analyse de risque d’un système d’information dédié à la vidéoprotection
- Identification des mesures de sécurité ressortant de cette analyse de risque applicable au réseau du système
- Mise en œuvre de ces mesures sur une plateforme de test composée d’une part des matériels et logiciels généralement utilisés par l’entreprise dans les systèmes de sécurité qu’elle propose à ses clients et d’autre part des matériels et logiciels nécessaires à la mise en place des mesures de sécurité

2. Analyse de risques

Identifier les besoins de sécurité des systèmes de vidéoprotection est la première étape du projet. Cette étape est réalisée via la conduite d'une analyse de risque informatique. Des mesures de sécurité pourront ainsi être mises en place afin de réduire ou supprimer les risques mis en évidence.
L'analyse de risque est réalisée via la méthode EBIOS Risk Manager (EBIOS RM).

2.1. Objectifs de la sécurité des systèmes d'information

Les systèmes d'information sont conçus dans le but de créer, traiter, stocker et faire circuler des données. Ces données représentent une grande valeur pour les entreprises, elles sont en effet souvent sources d'investissements en termes de recherche et développement, de savoir faire ou même d'acquisition d'informations. Leurs protection est même parfois soumise à des obligations règlementaires. Assurer la sécurité de ces données est donc essentielle et se caractérise en termes de [Ghernaouti - 2019] :

- Confidentialité : cette notion est liée au fait que l'accès à la donnée ne doit être possible que par les personnes dument autorisées. Des mécanismes peuvent être mis en place pour garantir cette confidentialité, comme le chiffrement des données ou la limitation et le contrôle des accès.
- Intégrité : ce critère repose sur la garantie que la donnée est intacte, c'est-à-dire qu'elle n'a pas été modifiée ou supprimée à l'insu de son propriétaire. L'intégrité est souvent contrôlée grâce à des mécanismes de chiffrement ou de signature des données.
- Disponibilité : ce critère défini le fait que la donnée doit être accessible et utilisable quand on en a besoin. Des mesures techniques peuvent également être mise en place pour garantir cette disponibilité, comme la redondance des systèmes ou les plans de sauvegarde qui permettent de restaurer les données en cas d'indisponibilité.

Un dernier critère, qui s'impute de manière implicite aux trois autres, est le critère de traçabilité. En effet il est primordial dans un système d'information de connaitre qui est à l'origine de la création, de la modification ou de la suppression de la donnée et ainsi éventuellement qui est à l'origine de sa perte de confidentialité, d'intégrité ou de disponibilité. Ce critère est également appelé imputabilité et non-répudiation.

2.2. La méthode EBIOS Risk Manager

EBIOS Risk Manager est la méthode d'appréciation et de traitement des risques éditée par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Elle est applicable à n'importe quelle organisation aussi bien publique que privée sans préférence de taille ou de secteur d'activité. Elle est utilisée pour les systèmes d'informations déjà en fonctionnement ou dont l'élaboration est en cours.

EBIOS RM propose une approche de gestion du risque numérique en deux temps, représentée graphiquement par la pyramide de management du risque :

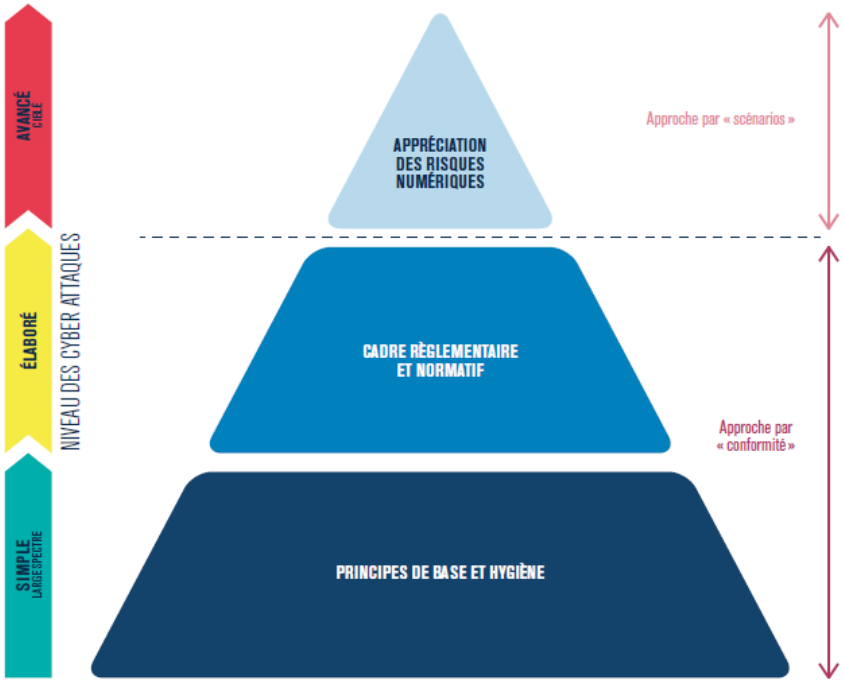

Figure 4 : Pyramide de management du risque

Cette pyramide met en évidence que tout système d'information doit d'abord reposer sur une base constituée du respect des règles d'hygiène informatique et de la conformité aux référentiels applicables. Ensuite, une approche par scénarios permettra d'évaluer de façon avancée les risques et menaces pesant sur le système d'information étudié.

Pour cela cette méthode, dite « itérative », s'organise en la réalisation successive de cinq ateliers :

1) **Cadrage et socle de sécurité :**

Le premier atelier permet de définir l'objet de l'étude et le socle de sécurité. Il s'agit d'identifier les biens à protéger ainsi que les référentiels applicables au système étudié afin de lister les mesures de sécurités qui y sont préconisées.

2) **Sources de risque :**

Le second atelier vise à identifier et évaluer les sources de risque ainsi que leurs objectifs visés pour permettre de dresser la cartographie des risques.

3) **Scénarios stratégiques :**

Le troisième atelier consiste à bâtir les scénarios stratégiques. Il s'agit de scénarios représentant les chemins d'attaque qu'une source de risque identifiée dans l'atelier précédant sera susceptible de suivre afin d'atteindre son objectif visé.

4) **Scénarios opérationnels :**

Le quatrième atelier sert à construire, sur la base des scénarios stratégiques écrits lors du troisième atelier, les scénarios opérationnels qui représentent les modes opératoires techniques qui seront certainement utilisés par les sources de risque.

5) **Traitement du risque :**

Enfin, le cinquième atelier a pour but de synthétiser l'ensemble des risques mis en évidences afin de définir une stratégie de traitement du risque.

Cette démarche, qui s'inscrit dans un plan d'amélioration continue de la sécurité, prévoit la mise en place des ateliers par la réalisation de deux cycles :

- Le cycle stratégique : cycle complet comprenant la réalisation de l'intégralité des ateliers de la méthode
- Le cycle opérationnel : cycle court consistant uniquement à la réalisation des ateliers 4 et 5

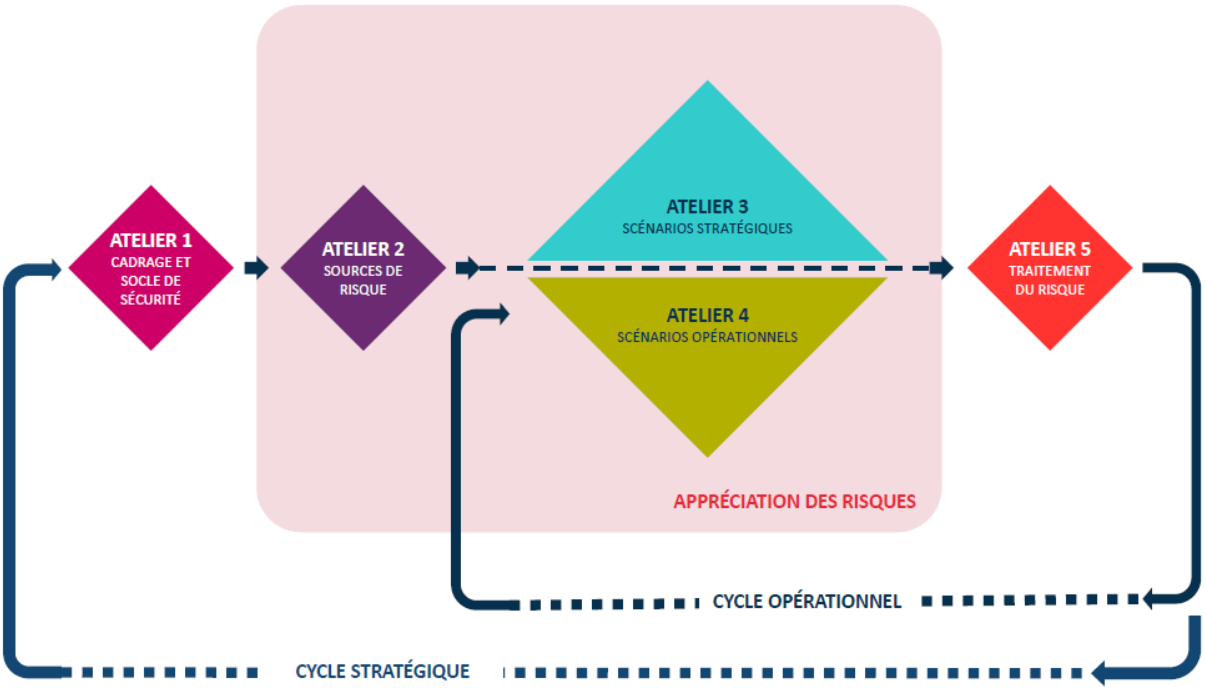

Figure 5 : Représentation graphique des ateliers et des cycles de la méthode EBIOS RM

La figure 5 ci-dessus représente la chronologie des ateliers et leurs inscriptions dans les deux cycles de la méthode. Si le cycle stratégique est à réaliser au complet une seule fois (à moins que le périmètre de l'étude change), le cycle opérationnel sera quant à lui répété de façon régulière, selon une période définie par l'organisation, afin de compléter les scénarios opérationnels en fonction des incidents de sécurité survenus et des nouvelles vulnérabilités ou modes opératoires identifiées.

2.3. Cadrage et socle de sécurité

La méthode EBIOS RM permet donc de conduire une analyse de risque complète en réalisant les différents ateliers proposés les uns à la suite des autres. En fonction de l'objectif final de cette analyse, il convient en premier lieu d'adapter la liste des ateliers à réaliser. En effet EBIOS RM propose une grille permettant de connaitre la liste des ateliers à conduire en fonction de l'objectif visé :

Tableau I : Ateliers EBIOS RM à conduire en fonction de l'objectif de l'étude

	Ateliers à conduire				
Objectif de l'étude	**1**	**2**	**3**	**4**	**5**
Identifier le socle de sécurité adapté à l'objet de l'étude	**X**				
Être en conformité avec les référentiels de sécurité numérique	**X**				**X**
Évaluer le niveau de menace de l'écosystème vis-à-vis de l'objet de l'étude			**X**		
Identifier et analyser les scénarios de haut niveau, intégrant l'écosystème		**X**	**X**		
Réaliser une étude préliminaire de risque pour identifier les axes prioritaires d'amélioration de la sécurité	**X**	**X**	**X**		**X**
Conduire une étude de risque complète et fine, par exemple sur un produit de sécurité ou en vue de l'homologation d'un système	**X**	**X**	**X**	**X**	**X**
Orienter un audit de sécurité et notamment un test d'intrusion			**X**	**X**	
Orienter les dispositifs de détection et de réaction, par exemple au niveau d'un centre opérationnel de la sécurité (SOC)			**X**	**X**	

Le tableau I ci-dessus, extrait du guide de la méthode EBIOS RM [ANSSI - 2018a], indique que dans le cadre de la conduite d'une étude de risque préliminaire pour déterminer les mesures de sécurité prioritaires (cadre orange dans le tableau), il convient de réaliser les ateliers 1, 2, 3 et 5. Il s'agit alors de mener une itération du cycle stratégique sans entrer dans le détail technique des scénarios opérationnels.

2.3.1. Cadre de l'étude

La présente analyse a pour objectifs :

- d'identifier les risques informatiques pesant sur un système d'information dédié à la vidéoprotection
- d'identifier les mesures de sécurités à mettre en œuvre pour traiter ces risques

L'étude est réalisée en se plaçant du point de vue de l'utilisateur du système, autrement dit le client de Securitas Sécurité Electronique, qui sera désigné comme étant « l'organisation ». L'entreprise Securitas Sécurité Electronique sera quant à elle désigné « le prestataire d'installation et de maintenance du système ».

L'étude se focalise sur le système d'information en posant l'hypothèse que ce dernier est isolé et ne sera donc pas interconnecté avec un autre système d'information (privé ou publique).

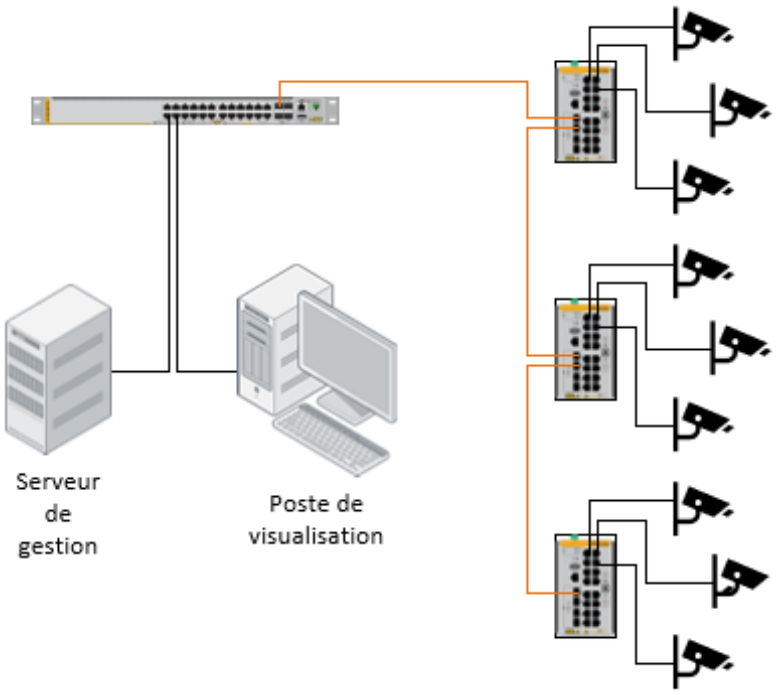

Figure 6 : Cartographie technique du système

La figure 6 ci-dessus représente le périmètre technique de l'étude. Le système est composé d'un réseau informatique support, de caméras IP ainsi que d'un serveur de gestion et d'un poste de visualisation. Cette cartographie est représentative des systèmes d'information dédié à la sécurité d'un site qu'installe généralement Securitas Sécurité Electronique.

Au-delà des différents composants nécessaires au fonctionnement du système de vidéoprotection, il est également important de prendre en compte leurs implantations physiques

sur les sites équipés. En effet dans un système d'information classique les équipements sont généralement installés et utilisés dans des environnements protégés du site. Les locaux techniques servent à abriter les serveurs et les commutateurs réseaux et les postes des utilisateurs sont quant à eux utilisés dans les locaux accessibles uniquement aux collaborateurs de l'organisation.

Dans le système de vidéoprotection, les besoins de positionnement des caméras IP résultant des besoins de surveillance du site nécessitent d'installer ces équipements dans des zones semi-publiques voir publiques (extérieurs du site). De plus les contraintes en termes de longueur maximale admissible de câble réseau impose également l'installation d'une partie des commutateurs constituant le réseau dans ces zones semi-publiques.

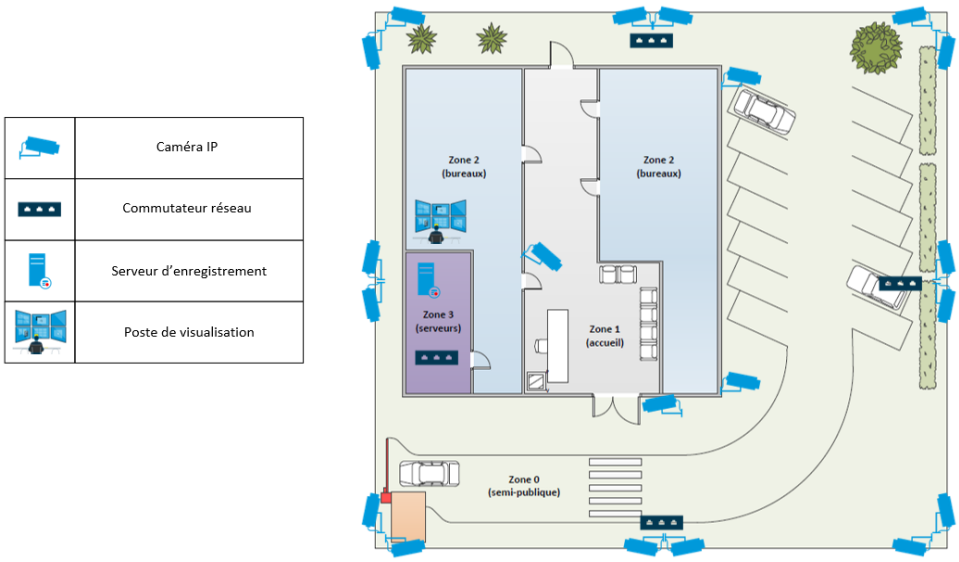

Figure 7 : Répartition géographique des équipements du système de vidéoprotection

La figure 7 ci-dessus représente l'implantation physique des différents équipements du système de vidéoprotection sur un site. Même si les serveurs d'enregistrements et les postes de visualisation sont installés dans des zones protégées (non accessible au public), une partie des caméras IP et des commutateurs réseaux sont eux installés en zone semi-publique.

2.3.2. Périmètre métier et technique

En premier lieu il est nécessaire de recenser la mission principale du système d'information, les valeurs métiers et les biens supports associés [ANSSI - 2018a].

La mission principale permet de délimiter le cadre de l'analyse de risque. C'est la mission pour laquelle le système d'information est mis en œuvre.

Les valeurs métiers représentent les composantes importantes pour l'organisation nécessaires à la réalisation de la mission principale, qui peuvent être des processus ou des informations essentielles. Elles constituent le patrimoine informationnel qu'une source de risque devra attaquer pour atteindre ses objectifs.

Dans le cadre de cette étude, la mission principale est d'assurer la surveillance et la protection d'un site physique au travers d'un système de vidéoprotection. Cette surveillance s'exerce par l'exploitation de plusieurs valeurs métier.

On identifie premièrement l'exploitation en elle-même du système de vidéoprotection, qui repose sur les différents composants propres du système (caméras, serveurs de gestion…) ainsi que les opérateurs les utilisant. La seconde valeur métier mise en évidence sont les enregistrements vidéo stockés par le système, qui représentent une information capitale pour l'organisation. Enfin, la troisième valeur métier mise en évidence sont les fichiers journaux du système de vidéoprotection. En effet selon l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance, tout système de vidéoprotection doit posséder un journal des événements traçant l'intégralité des actions des opérateurs, comme les connexions et déconnexions des utilisateurs, les relectures et les extractions d'images ou les modifications des paramètres du système.

Les valeurs métiers doivent également être évaluées sur les trois critères de Confidentialité, Intégrité et Disponibilité. Pour cela, et selon les retours d'expérience de Securitas Sécurité Electronique dans les besoins généralement exprimés par ses clients, trois échelles sont définies, permettant chacune d'évaluer un besoin :

Tableau II : Echelle des besoins de confidentialité

Valeur	Description
4	La valeur métier ne doit être accessible qu'aux personnels habilités et ayant le besoin d'en connaître
3	La valeur métier ne doit être accessible qu'aux personnels autorisés et ayant le besoin d'en connaître
2	La valeur métier est interne à l'organisation et peut-être accessible à tous les collaborateurs ou parties prenantes
1	La valeur métier est publique

Tableau III : Echelle des besoins d'intégrité

Valeur	Description
4	La valeur métier doit être rigoureusement intègre
3	La valeur métier peut ne pas être intègre, si l'altération est identifiée et l'intégrité de la valeur métier retrouvée
2	La valeur métier peut ne pas être intègre si l'altération est identifiée.
1	La valeur métier semble être intègre mais est en réalité altérée

Tableau IV : Echelle des besoins de disponibilité

Valeur	Description
4	La valeur métier doit être disponible dans les 4h
3	La valeur métier doit être disponible dans les 24h
2	La valeur métier doit être disponible dans les 72h
1	La valeur métier peut être indisponible plus de 72h

Les valeurs métiers retenues sont listées dans le tableau V et elles sont associées à leurs évaluations en termes de confidentialité (C), intégrité (I) et disponibilité (D) :

Tableau V : Liste des valeurs métier et évaluation CID

Valeurs métier					
Id	**Nom**	**Description**	**Besoins de sécurité**		
			C	**I**	**D**
VM1	Exploitation du système de vidéoprotection	Eléments physiques et organisationnels sur lesquels repose la gestion de la sécurité du site par l'exploitation en direct des flux vidéo	**4**	**4**	**4**
VM2	Enregistrements vidéo	Flux vidéo enregistrés	**4**	**4**	**2**
VM3	Fichiers journaux	Journal des événements du système	**3**	**4**	**4**

Les biens supports sont quant à eux les éléments du système d'information sur lesquels reposent la valeur métier qui leurs est associée. Ces éléments peuvent être physiques (locaux de l'organisation), numériques (serveurs, logiciels, base de données) ou organisationnels (collaborateurs). Les mesures de sécurité devront s'appliquer sur ces biens supports.

Les biens supports retenus sont les suivants :

Tableau VI : Liste des biens support associés aux valeurs métier

Biens supports			
Id	**Nom**	**Description**	**Valeur métier associée**
BS1	Caméras IP	Dispositif de prise d'images	VM1
BS2	Postes de visualisation	PC client du serveur de gestion servant à la visualisation en direct ou en relecture distante des images des caméras IP de surveillance	
BS3	Réseau support	Réseau informatique composé des différentes liaisons (cuivre, optiques) et équipements (commutateurs) servant à transmettre les informations entre les composants du système	
BS4	Serveurs de gestion	Serveurs informatiques permettant la gestion du système et le stockage des images sur lesquels est installé le VMS	
BS5	Opérateurs	Employés en charge de l'exploitation du système de vidéoprotection	
BS6	Base de données des enregistrements	Base de données contenant les enregistrements des caméras de vidéoprotection	VM2
BS7	Base de données des journaux	Base de données contenant le journal des événements du système	VM3

La synthèse des éléments précédemment définis est représentée dans le tableau VII :

Tableau VII : Synthèse valeurs métier et biens supports associés

Mission	**Assurer la surveillance d'un site**						
Valeur Métier	Exploitation du système de vidéoprotection					Enregistrements vidéo	Fichiers journaux
Nature	Processus					Information	Information
Description	Eléments physiques et organisationnels sur lesquels repose la gestion de la sécurité du site par l'exploitation en direct des flux vidéo					Flux vidéo enregistrés	Journal des événements du système
Entité responsable	Service de sécurité du site					Service de sécurité du site	Service de sécurité du site
Bien Support	Caméras IP	Postes de visualisation	Réseau	Serveurs de gestion	Opérateurs	Base de données des enregistrements	Base de données des journaux
Description	Dispositif de prise d'images	PC client du serveur de gestion servant à la visualisation en direct ou en relecture distante des images des caméras IP	Réseau informatique composé des différentes liaisons (cuivre, optiques) et équipements (commutateurs) servant à transmettre les informations entre les composants du système	Serveurs informatiques permettant la gestion du système et le stockage des images sur lesquels est installé le VMS	Employés en charge de l'exploitation du système de vidéoprotection	Base de données contenant les enregistrements des caméras de vidéoprotection	Base de données contenant le journal des événements du système
Entité responsable	Service de sécurité du site	Service de sécurité du site	Service de sécurité du site	Service de sécurité du site	Responsable sécurité du site	Service de sécurité du site	Service de sécurité du site

2.3.3. Socle de sécurité

Au regard du périmètre métier et technique de l'étude, les référentiels suivants ont été retenus pour établir le socle de sécurité du système :

Tableau VIII : Liste des référentiels applicables

Id	Référentiel	Rédacteur	Version
Réf 1	Guide d'hygiène informatique	ANSSI	2.0
Réf 2	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection	ANSSI	2.0
Réf 3	Référentiel APSAD D32 Cybersécurité	APSAD	Juin 2017

Le guide d'hygiène informatique de l'ANSSI [ANSSI - 2017] a été publié initialement en 2013 et mis à jour en 2017. Il décrit un ensemble de mesures de sécurité applicables aux systèmes d'information en général. Ces mesures sont issues de l'expérience de l'ANSSI en fonction des constats fait lors de ses différentes interventions à la suite d'attaques informatiques. L'ANSSI part du principe que si les mesures que ce référentiel décrit avaient été appliquées, la majeure partie de ces attaques auraient pu être évitées. Le guide énumère 42 mesures de sécurité d'ordres organisationnelles ou techniques. Elles seront retenues en fonction de leurs pertinences et applicabilités à l'objet de l'étude.

Le guide de recommandation sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection [ANSSI - 2020a] , également publié par l'ANSSI, dresse quant à lui des mesures de sécurité spécifiquement étudiées pour ces systèmes. Sa version initiale date de 2012 et il est actuellement dans sa version 2.0 datant de mars 2020. Les mesures de sécurité listées sont au nombre de 91, mesures qui seront également retenues en fonction de l'objet de l'étude.

Le Centre National de la Prévention et de la Protection (CNPP), qui délivre les certifications APSAD, a également publié un guide traitant de la cybersécurité des systèmes de sécurité, le référentiel D32 [CNPP - 2017]. Les certifications APSAD sont délivrés aux entreprises installant des systèmes de sécurité (R81 pour les systèmes de détection intrusion, D83 pour les systèmes de contrôle d'accès, R82 pour les systèmes de vidéoprotection) et sont gages de qualité dans l'installation de ces systèmes. L'entreprise Securitas Sécurité Electronique étant

déjà certifiée APSAD R81, R82 et D83, il est tout naturel que les systèmes qu'elle installe suivent les recommandations du référentiel en vue d'être à l'avenir certifié APSAD D32.
Les mesures de sécurité listées dans ces documents sont de trois types :

- Organisationnelles : ces mesures seront mises en place par l'organisation en établissant des procédures spécifiques, des chartes ou des règles d'utilisation informatique, des formations techniques ou de sensibilisation de ses collaborateurs. Il s'agit également de mettre en place une démarche d'amélioration continue de la sécurité du système d'information, en planifiant des audits réguliers et des mises à jour du système en conséquence.

- Physiques : les mesures de sécurité physiques s'appliqueront sur les modes d'installation ou de protection physique des composants du système d'information, comme par exemple le fait d'installer les éléments clés du système d'information (serveurs, commutateurs, systèmes de sauvegarde…) dans les locaux protégés aux accès limités.

- Techniques : les mesures techniques seront quant à elles appliquées par l'utilisation de matériels ou logiciels spécifiques, du durcissement de la configuration des équipements et de l'utilisation de protocoles sécurisés.

Les mesures de sécurités retenues, identifiées par référentiel source, sont les suivantes :

Tableau IX : Liste des mesures de sécurité organisationnelles

Référentiel source	Mesure de sécurité
Réf 1	Former les équipes opérationnelles à la sécurité des systèmes d'information
Réf 1	Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique
Réf 1	Maitriser les risques de l'infogérance
Réf 1	Maintenir à jour une cartographie du système d'information
Réf 1	Maintenir à jour un inventaire des comptes utilisateurs privilégiés
Réf 1	Mettre en place des procédures d'arrivée et de départ des utilisateurs
Réf 1	Autoriser la connexion au réseau de l'entité aux seuls équipements maîtrisés
Réf 1	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques
Réf 1	Définir une politique de mise à jour des composants du système d'information
Réf 1	Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles
Réf 1	Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives associées
Réf 2	Définir les processus organisationnels liés à la gestion de la vidéoprotection
Réf 2	Mener une réflexion sur le niveau de continuité de service souhaité
Réf 2	Distinguer les postes d'administration des postes d'utilisation métier
Réf 2	Assurer le maintien en condition de sécurité
Réf 2	Contrôler minutieusement les dispositifs en panne contenant des éléments cryptographiques avant réparation ou mise au rebut
Réf 2	Veiller à disposer d'un contrat de maintenance ou d'une organisation de maintenance interne assurant le remplacement du dispositif défaillant
Réf 2	Éviter de mettre en place une solution de télémaintenance
Réf 3	Mettre en place un plan de continuité d'activité testé et fonctionnel

Tableau X : Liste des mesures de sécurité physiques

Référentiel source	Mesure de sécurité
Réf 1	Contrôler et protéger l'accès aux salles serveurs et aux locaux techniques
Réf 2	Protéger les liaisons filaires, notamment celles circulant en extérieur
Réf 2	Ne pas laisser les points d'accès au réseau apparents

Tableau XI : Liste des mesures de sécurité techniques

Référentiel source	Mesure de sécurité
Réf 1	Créer des comptes utilisateurs et administrateurs nominatifs
Réf 1	Attribuer les bons droits sur les ressources sensibles du système d'information
Réf 1	Définir et vérifier des règles de choix et de dimensionnement des mots de passe
Réf 1	Protéger les mots de passe stockés sur les systèmes
Réf 1	Changer les éléments d'authentification par défaut sur les équipements et services
Réf 1	Activer et configurer le pare-feu local des postes de travail
Réf 1	Segmenter le réseau et mettre en place un cloisonnement entre ces zones
Réf 1	Utiliser des protocoles sécurisés dès qu'ils existent
Réf 1	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information
Réf 1	Limiter au strict besoin opérationnel les droits d'administration sur les postes de travail
Réf 1	Activer et configurer les journaux des composants les plus importants
Réf 2	Cloisonner physiquement ou logiquement les SI
Réf 2	Privilégier une connectivité filaire pour les dispositifs de vidéoprotection
Réf 2	Cloisonner logiquement par type les dispositifs au sein du réseau support
Réf 2	Désactiver les ports inutilisés sur les commutateurs réseau
Réf 2	Contrôler les accès aux ports réseau par authentification ou à minima par vérification des adresses MAC
Réf 2	Cloisonner logiquement le réseau des caméras extérieures
Réf 2	Filtrer les flux entre les réseaux
Réf 2	Chiffrer et authentifier les flux émis et reçus par les caméras
Réf 2	Mettre en place une infrastructure de gestion de clés
Réf 2	Remplacer les mots de passe par défaut des caméras
Réf 2	Remplacer les certificats installés par défaut dans les équipements
Réf 2	Désactiver les fonctions d'administration non utilisées
Réf 2	Sécuriser le SI de vidéoprotection
Réf 2	Synchroniser les horloges des équipements sur une source de temps fiable
Réf 2	Privilégier les solutions d'authentification et de chiffrement non-propriétaires
Réf 2	Privilégier les solutions de vidéoprotection proposant un bon niveau de maturité en matière de sécurité numérique
Réf 2	Effectuer des sauvegardes régulières
Réf 3	Dédié physiquement ou logiquement le réseau au système de sécurité
Réf 3	Désactiver les protocoles obsolètes (telnet, ftp…)
Réf 3	Activer la journalisation des systèmes

2.3.4. Evénements redoutés

Les événements redoutés sont associés aux valeurs métier identifiés précédemment. Il s'agit de faits qui, s'ils se produisaient, mettraient en péril l'activité de l'organisation.

Pour les identifier, il est nécessaire de mener une réflexion sur les effets indésirables que pourrait porter l'atteinte à la confidentialité, à l'intégrité ou à la disponibilité de la valeur métier ou, dans son ensemble, à la capacité pour le système d'information de réaliser la mission pour laquelle il a été conçu [ANSSI - 2018a].

Une fois listés, il s'agit de caractériser les événements redoutés selon deux critères. Tout d'abord, les événements redoutés vont avoir, s'ils se produisent, un ou plusieurs impacts sur l'organisation. Les différentes catégories d'impact proposées par l'ANSSI sont les suivantes [ANSSI - 2018b] :

- Impacts sur la mission : incapacité à fournir tout ou partie du service pour lequel le système d'information est conçu.
- Impacts humains, matériels ou environnementaux : mise en danger des personnes, des biens ou de l'environnement.
- Impacts sur la gouvernance : incapacité de prise de décision pour le pilotage de l'organisation, perte de confiance ou tension des collaborateurs, perte de patrimoine scientifique ou technique de l'organisation.
- Impacts financiers : perte de chiffre d'affaires ou de marchés, engendrement de dépenses imprévues.
- Impacts juridiques : procès, amende ou condamnation de l'organisation ou de l'un de ses membres dirigeants.
- Impacts sur l'image et la confiance : publication d'articles de presse négatifs, perte de crédibilité vis-à-vis des clients, des usagers ou des actionnaires de l'organisation.

Ensuite, les événements redoutés vont être caractérisés par leurs gravités. Pour les évaluer il est nécessaire d'établir une échelle de gravité :

Tableau XII : Echelle de gravité des événements redoutés

Echelle de gravité	Description
4 - Critique	Incapacité totale pour l'organisation d'assurer la sécurité du site, mise en danger des personnes et des biens. Fuite de savoir-faire ou espionnage de l'organisation.
3 - Grave	Forte dégradation de la capacité de l'organisation à assurer la sécurité du site, mise en danger d'une partie des personnes et des biens. Incapacité à prouver des faits via l'incapacité d'accès aux enregistrements ou au fichiers journaux.
2 - Significative	Dégradation limitée de la capacité de l'organisation à assurer la sécurité du site, potentielle mise en danger d'une partie des personnes et des biens.
1 - Négligeable	Faible dégradation de la capacité de l'organisation à assurer la sécurité du site, aucun impact sur la sécurité des biens et des personnes.

Dans le cadre du système d'information dédié à la vidéoprotection, les événements redoutés sont tournés vers la perte de confidentialité des flux vidéo des caméras, qu'ils soient en direct ou enregistrés, mais également vers la perte d'intégrité ou de disponibilité de ces derniers. On note également comme événement redouté important la perte de disponibilité ou d'intégrité du journal des événements du système.

Il est possible, grâce à l'échelle établie, d'évaluer la gravité de l'événement redouté. Les événements les plus graves sont évidemment ceux remettant en cause la disponibilité totale du service mais également la perte de confidentialité, même partielle, des données qu'il gère et stocke.

Les événements redoutés sont ainsi identifiés et caractérisés, l'échelle de gravité et l'évaluation de la gravité de chaque événement ayant été réalisée selon les retours d'expérience de Securitas Sécurité Electronique :

Tableau XIII : Liste des événements redoutés associés à leurs impacts et leur gravité

Id	Valeur Métier	Evénement Redouté	Catégories d'impact	Gravité
ER1	VM1	Le flux vidéo en direct d'une caméra est indisponible ou n'est pas intègre	Impacts sur la mission	**1**
ER2	VM1	Le flux vidéo en direct de plusieurs caméras est indisponible ou n'est pas intègre	Impacts sur la mission Impacts humains et/ou matériels	**2**
ER3	VM1	Le flux vidéo en direct de toutes les caméras est indisponible ou n'est pas intègre	Impacts sur la mission Impacts humains et/ou matériels Impacts juridiques	**4**
ER4	VM1	Le flux vidéo en direct d'une ou plusieurs caméras est accessible publiquement ou à un tier non autorisé	Impacts sur la gouvernance Impacts juridiques Impacts sur l'image et la confiance	**4**
ER5	VM2	Les enregistrements des flux vidéo sont supprimés ou leur intégrité est altérée	Impacts sur la mission Impacts juridiques Impacts sur l'image et la confiance	**3**
ER6	VM2	Les enregistrements vidéo sont indisponibles plus de 72h	Impacts sur la mission Impacts juridiques Impacts sur l'image et la confiance	**3**
ER7	VM2	La capacité d'enregistrement des flux vidéo est indisponible pendant plus de 24h	Impacts sur la mission Impacts sur la gouvernance Impacts juridiques Impacts sur l'image et la confiance	**4**
ER8	VM2	Les enregistrements vidéo sont accessibles publiquement ou à un tier non autorisé	Impacts sur la gouvernance Impacts juridiques Impacts sur l'image et la confiance	**4**
ER9	VM3	Le journal des événements est supprimé ou son intégrité est altérée	Impacts sur la mission Impacts juridiques	**3**

2.4. Sources de risque et objectifs visés

Le second atelier de la méthode EBIOS RM consiste à identifier les sources de risque (SR) associées à leurs objectifs visés (OV).

Les données d'entrée de cet atelier sont les éléments de sortie du premier atelier, soit les valeurs métiers et les événements redoutés. Les données de sortie sont les couples SR/OV retenus ou mis sous surveillance.

2.4.1. Sources de risque

Une source de risque est une personne, un groupe de personnes ou une typologie de personnes (administrateurs, utilisateurs, attaquant) qui est susceptible de présenter un risque pour une valeur métier.

Selon l'ANSSI [ANSSI - 2018b], les catégories de sources de risque peuvent être :

- Etatique : source de risque émanant des états ou services de renseignement étrangers, groupe professionnel d'attaquant disposant de moyens réputés illimités et pouvant mener des attaques sur des temps relativement long à des fins d'espionnage ou de vol d'informations
- Crime organisé : organisations mafieuses aux moyens conséquents, menant la plupart du temps des attaques, de plus en plus sophistiquées, à but lucratives
- Concurrent : organisations concurrentes aux ressources importantes et opérant dans le même secteur d'activité, dont le vol d'information représenterait une économie importante en termes de recherche et développement
- Terroriste : groupe d'attaquant disposant de moyens importants, réalisant des attaques généralement peu sophistiquées mais avec une grande détermination afin de rendre indisponible un service
- Activiste idéologique : groupe d'attaquant, à l'image des cyber-terroristes, réalisant des attaques généralement peu sophistiquées mais avec une grande détermination afin de véhiculer une idéologie
- Officine spécialisée : groupe d'attaquant chevronnés monnayant ses services pour réaliser des attaques ou créant et vendant des kits d'attaques

- Amateur : attaquant aux moyens très limités, agissant le plus souvent par recherche de l'exploit en utilisant des scripts disponibles en ligne
- Vengeur : attaquant motivé par un esprit de vengeance, par exemple un ancien collaborateur de l'organisation licencié, disposant de peu de moyens mais parfois d'une connaissance importante du système auquel il désire s'attaquer
- Malveillant pathologique : attaquant n'ayant d'autre but que l'envie de nuire, parfois pour l'appât du gain, et disposant de moyens très limités

Les sources de risque retenues sont les suivantes, la justification est donnée pour chaque source de risque en lien avec ce que possède l'organisation qui pourrait être un intérêt pour cette source :

Tableau XIV : Liste des sources de risque

Sources de Risque			
Id	**Source de Risque**	**Catégorie**	**Justification**
SR1	Etat étranger	Etatique	Organisation servant l'état dont les informations et/ou le savoir-faire pourraient intéresser des états étrangers
SR2	Concurrent	Concurrent	Organisation à fort potentiel scientifique et technique dont le savoir-faire pourrait intéresser ses concurrents
SR3	Crime organisé	Crime organisé	Organisation aux moyens financiers importants attirant les convoitises des groupes mafieux aux buts lucratifs (chantage)
SR4	Ex-collaborateur	Vengeur	Organisation aux ressources humaines importante augmentant les probabilités de collaborateur mécontent
SR5	Activiste	Activiste idéologique	Organisation dont les activités dépendent du secteur de la défense ayant de nombreux opposant idéologiques

2.4.2. Objectifs visés

L'objectif visé est le but à atteindre par la source de risque. L'objectif visé ne porte pas toujours directement sur une valeur métier, mais il impliquera nécessairement pour sa réalisation l'accomplissement d'un ou plusieurs événements redoutés.

Selon l'ANSSI [ANSSI - 2018b], les catégories d'objectifs visés peuvent être :

- Espionnage : l'objectif est ici le vol d'information ou de potentiel scientifique et technique, généralement effectué sur une longue période
- Pré-positionnement stratégique : la finalité de cet objectif n'est pas clairement définie, mais consiste à bénéficier d'un accès au système pour pouvoir le piloter le moment souhaité (par exemple constitution d'un réseau de machine zombie pour s'en servir dans de futures attaques)
- Influence : le but est ici la diffusion de fausses informations afin de nuire à la réputation de l'organisation visée, par exemple par la modification de son site internet
- Entrave au fonctionnement : sabotage du système afin d'altérer son fonctionnement ou le rendre entièrement inopérable
- Lucratif : le gain financier est ici visé, actuellement cet objectif est la plupart du temps réalisé via la diffusion de rançongiciel ou le vol d'informations qui seront échangées contre une rançon
- Défi : l'objectif est ici de réaliser une attaque dans le seul but de l'amusement ou du défi en vue de reconnaissance sociale

Les objectifs visés retenus sont les suivants, ils sont chacun associés à une ou plusieurs sources de risque mentionnées dans le tableau XIV page 35 et font également référence à un ou plusieurs événements redoutés listés dans le tableau XIII page 33 :

Tableau XV : Liste des objectifs visés

Objectifs Visés					
Id	**Objectif Visé**	**Catégorie**	**Sources de Risque**	**Description**	**Evénements Redouté**
OV1	Espionner l'intérieur du site	Espionnage	SR1 SR2	Espionner l'intérieur du site via les images de vidéoprotection pour voler des informations ou des procéder de fabrication	ER4 ER8
OV2	Obtenir une rançon	Lucratif	SR3	Rendre le système inopérant dans le but de demander une rançon pour le rendre disponible à nouveau	ER7
OV3	Pénétrer sur le site pour vol	Lucratif	SR3	Rendre les flux vidéo en direct des caméras indisponible pour pouvoir pénétrer sur le site sans être vue dans le but de commettre un vol	ER2 ER3
OV4	Pénétrer sur le site pour dégradation	Influence	SR5	Rendre les flux vidéo en direct des caméras indisponible pour pouvoir pénétrer sur le site sans être vue dans le but de commettre des dégradations	ER2 ER3
OV5	Supprimer les journaux	Entrave	SR4	Supprimer les journaux du système pour effacer des actions compromettantes	ER9
OV6	Supprimer les enregistrement	Entrave	SR4	Supprimer les enregistrements vidéo du système par vengeance	ER5
OV7	Rendre impossible les enregistrement	Entrave	SR3 SR4	Rendre indisponible les serveurs de gestion pour camoufler des actions malveillantes	ER5

2.4.3. Evaluation des couples SR/OV

La dernière étape de cet atelier consiste à dresser la liste des couples source de risque (SR) et objectif visé (OV) et d'évaluer la pertinence de chacun.

Une échelle est à nouveau nécessaire, celle-ci permet de déterminer la pertinence du couple SR/OV en fonction de la motivation et des ressources de la source de risque :

Tableau XVI : Echelle d'évaluation des couples SR/OV

		Ressources			
		Ressources limitées	**Ressources significatives**	**Ressources importantes**	**Ressources illimitées**
Motivation	**Fortement motivée**	Moyennement pertinent	Plutôt pertinent	Très pertinent	Très pertinent
	Assez motivée	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent	Très pertinent
	Peu motivée	Peu pertinent	Moyennement pertinent	Plutôt pertinent	Plutôt pertinent
	Très peu motivée	Peu pertinent	Peu pertinent	Moyennement pertinent	Moyennement pertinent

Dans le tableau XVI ci-dessus, les ressources représentent aussi bien la capacité financière que le niveau de compétence cyber mais également la capacité humaine et le temps dont dispose la source de risque pour réaliser son attaque. La motivation est évaluée en fonction de l'intérêt qu'a la source de risque pour atteindre son objectif.

Une fois l'échelle établie, chaque couple source de risque et objectif visé est alors répertorié et se voit appliquer une cotation en fonction de sa motivation et de ses ressources.

Comme vue précédemment, un état étranger disposera de ressources illimitées ainsi qu'une forte motivation. On peut également supposer qu'un concurrent de l'organisation sera une entreprise importante et disposera donc de ressources en conséquence et sera assez motivé pour atteindre son objectif. Le crime organisé sera quant à lui fortement motivé et disposera aussi de ressources importantes. Concernant l'ex-collaborateur, ses ressources seront limitées mais on peut supposer qu'il sera assez motivé. Enfin, l'activiste disposera également de ressources limitées bien qu'ayant une forte motivation.

Tous les éléments sont répertoriés dans le tableau XVII ci-dessous et la pertinence est ainsi évaluée :

Tableau XVII : Liste des couples SR/OV évalués selon leur pertinence

Couples SR/OV				
Identification		**Cotation**		**Pertinence**
Source de risque	**Objectif Visé**	**Motivation**	**Ressources**	
SR1 - Etat étranger	OV1 - Espionner l'intérieur du site	Fortement motivée	Ressources illimitées	**Très pertinent**
SR2 - Concurrent	OV1 - Espionner l'intérieur du site	Assez motivée	Ressources importantes	**Plutôt pertinent**
SR3 - Crime organisé	OV2 - Obtenir une rançon	Fortement motivée	Ressources importantes	**Très pertinent**
SR3 - Crime organisé	OV3 - Pénétrer sur le site pour vol	Fortement motivée	Ressources importantes	**Très pertinent**
SR3 - Crime organisé	OV7 - Rendre impossible les enregistrement	Fortement motivée	Ressources importantes	**Très pertinent**
SR4 - Ex-collaborateur	OV5 - Supprimer les journaux	Assez motivée	Ressources limitées	**Moyennement pertinent**
SR4 - Ex-collaborateur	OV6 - Supprimer les enregistrement	Assez motivée	Ressources limitées	**Moyennement pertinent**
SR4 - Ex-collaborateur	OV7 - Rendre impossible les enregistrement	Assez motivée	Ressources limitées	**Moyennement pertinent**
SR5 - Activiste	OV4 - Pénétrer sur le site pour dégradation	Fortement motivée	Ressources limitées	**Moyennement pertinent**

Pour la suite de l'étude, ne seront retenus que les couples SR/OV les plus pertinents, en l'occurrence l'état étranger ou le concurrent de l'organisation avec pour objectif d'espionner le site, mais aussi le crime organisé avec pour objectifs d'obtenir une rançon, de pénétrer sur le site pour effectuer un vol ou de rendre les enregistrements vidéo impossible.

Il convient ensuite de rapprocher les couples SR/OV retenus aux événements redoutés listés dans le tableau XIII page 33, on obtient alors la liste des couples SR/OV retenus associés aux événements redoutés identifiés les plus graves :

Tableau XVIII : Couples SR/OV retenus associés aux événements redoutés les plus graves

Couples SR/OV et événements redoutés				
Source de risque	**Objectif Visé**	**Pertinence**	**Evénement redouté**	**Gravité**
SR1 - Etat étranger	OV1 - Espionner l'intérieur du site	**Très pertinent**	ER4 - Le flux vidéo en direct d'une ou plusieurs caméras est accessible publiquement ou à un tier non autorisé	**4**
			ER 8 - Les enregistrements vidéo sont accessibles publiquement ou à un tier non autorisé	**4**
SR2 - Concurrent	OV1 - Espionner l'intérieur du site	**Plutôt pertinent**	ER4 - Le flux vidéo en direct d'une ou plusieurs caméras est accessible publiquement ou à un tier non autorisé	**4**
			ER8 - Les enregistrements vidéo sont accessibles publiquement ou à un tier non autorisé	**4**
SR3 - Crime organisé	OV2 - Obtenir une rançon	**Très pertinent**	ER7 - La capacité d'enregistrement des flux vidéo est indisponible pendant plus de 24h	**4**
SR3 - Crime organisé	OV3 - Pénétrer sur le site pour vol	**Très pertinent**	ER3 - Le flux vidéo en direct de toutes les caméras est indisponible ou n'est pas intègre	**4**
SR3 - Crime organisé	OV7 - Rendre impossible les enregistrement	**Très pertinent**	ER7 - La capacité d'enregistrement des flux vidéo est indisponible pendant plus de 24h	**4**

2.5. Scénarios stratégiques

Le troisième atelier de la méthode EBIOS RM consiste à élaborer les scénarios stratégiques en fonction des éléments définis dans les deux premiers ateliers. Il s'agit ici de s'intéresser à l'environnement du système, nommé dans la méthode « écosystème », dont un attaquant pourrait se servir pour atteindre son objectif.

Les données d'entrée de cet atelier sont les éléments de sortie des deux premiers ateliers, soit les valeurs métiers, les événements redoutés et les couples SR/OV retenus. Les données de sortie sont la cartographie de menace de l'écosystème, les scénarios stratégiques ainsi que les mesures de sécurité retenues pour l'écosystème.

2.5.1. Cartographie de la menace

La première étape de cet atelier consiste à identifier et évaluer les parties prenantes critiques de l'écosystème.

Les parties prenantes sont des organismes internes ou externes à l'organisation, qui peuvent se classer en trois catégories :

- Client : clients ou usagers des produits ou services de l'organisation
- Partenaire : organisme travaillant en collaboration avec l'organisation, cela peut être par exemple un organisme de contrôle étatique comme l'ANSSI ou une université travaillant sur des recherches communes avec l'organisation
- Prestataire : fournisseurs ou prestataires de services de l'organisation, Securitas Sécurité Electronique se situe dans cette catégorie en tant que prestataire d'installation et de maintenance des systèmes de sécurité

Ces parties prenantes doivent être en lien avec la mission réalisée par le système d'information. Il ne s'agit pas de lister tous les clients, partenaires et prestataires de l'organisation mais seulement ceux gravitant autour de l'objet de l'étude.

Les parties prenantes identifiés dans le cas du système de vidéoprotection sont les suivantes :

Tableau XIX : Liste des parties prenantes de l'écosystème

Description des parties prenantes			
Id	**Catégorie**	**Nom**	**Description**
P1	Partenaire	ANSSI/DRSD	Organisme de contrôle s'assurant du bon respect des règlementations en termes de systèmes de sécurité par l'organisation
F1	Prestataire	Prestataire d'entretien des locaux	Entreprise en charge de l'entretien (ménage) du site
F2	Prestataire	Prestataire de maintenance	Entreprise en charge de la maintenance des équipements du site, notamment les installations électriques
F3	Prestataire	Prestataire d'installation et de maintenance du système	Entreprise en charge de l'installation et de la maintenance du système de vidéoprotection

Pour évaluer les parties prenantes, il est nécessaire d'établir une échelle qui va permettre d'attribuer une évaluation sur quatre critères que sont :

- La dépendance : évaluation du niveau de dépendance vis-à-vis de la partie prenante
- La pénétration : évaluation du niveau de connaissance du système ainsi que du niveau d'accès logique et physique au système par la partie prenante
- La maturité cyber : évaluation des connaissances et du respect des règles de sécurité informatique de la partie prenante
- La confiance : évaluation du niveau de confiance de la partie prenante

Cette évaluation est faite en fonction de la connaissance que l'on a de la partie prenante dans ces différents critères, notamment dans les conditions présentes dans les contrats qui lient l'organisation à la partie prenante (par exemple, l'exigence d'une certification ISO 27001 dans le choix de son prestataire d'infogérance assurera un haut niveau de maturité cyber) et également à leurs conditions de travail imposées sur le site.

Une fois les quatre critères évalués, le niveau de menace de la partie prenante peut alors être calculé selon la formule suivante :

Niveau de menace = (Dépendance X Pénétration) / (Maturité cyber x Confiance)

L'échelle d'évaluation des critères des parties prenante est la suivante, elle est reprise en partie des fiches méthodes EBIOS RM [ANSSI - 2018b], seuls les degrés de pénétration ont été modifiés pour prendre en compte l'aspect accès physique aux locaux protégés :

Tableau XX : Echelle d'évaluation des parties prenantes

	Dépendance	Pénétration	Maturité Cyber	Confiance
1	Relation non nécessaire aux fonctions stratégiques.	Pas d'accès physique au local protégé. Pas d'accès logique aux données.	Des règles d'hygiène informatique sont appliquées ponctuellement et non formalisées. La capacité de réaction sur incident est incertaine.	Les intentions de la partie prenante ne peuvent être évaluées.
2	Relation utile aux fonctions stratégiques	Accès physique au local protégé en étant accompagné. Pas d'accès logique aux données.	Les règles d'hygiène et la réglementation sont prises en compte, sans intégration dans une politique globale. La sécurité numérique est conduite selon un mode réactif.	Les intentions de la partie prenante sont considérées comme neutres.
3	Relation indispensable mais non exclusive.	Accès physique au local protégé. Accès à toutes les données avec privilèges de type utilisateur.	Une politique globale est appliquée en matière de sécurité numérique. Celle-ci est assurée selon un mode réactif, avec une recherche de centralisation et d'anticipation sur certains risques.	Les intentions de la partie prenante sont connues et probablement positives.
4	Relation indispensable et unique (pas de substitution possible à court terme).	Accès physique au local protégé. Accès à toutes les données avec privilèges de type administrateur.	La partie prenante met en œuvre une politique de management du risque. La politique est intégrée et se réalise de manière proactive.	Les intentions de la partie prenante sont parfaitement connues et pleinement compatibles avec celles de l'organisation étudiée.

A l'aide de l'échelle précédente, les parties prenantes sont ainsi évaluées et leur niveau de menace calculé :

Tableau XXI : Evaluation initiale des parties prenantes

Evaluation des parties prenantes						
Catégorie	**Nom**	**Dépendance**	**Pénétration**	**Maturité Cyber**	**Confiance**	**Niv. De Menace**
Partenaire	P1 - ANSSI/DRSD	4	3	4	4	**0,75**
Prestataire	F1 - Prestataire d'entretien des locaux	1	2	1	2	**1**
Prestataire	F2 - Prestataire de maintenance	2	3	2	2	**1,5**
Prestataire	F3 - Prestataire d'installation et de maintenance du système	3	4	3	3	**1,33**

Le niveau de menace de chaque partie prenante est ensuite représenté graphiquement sur la cartographie de la menace initiale :

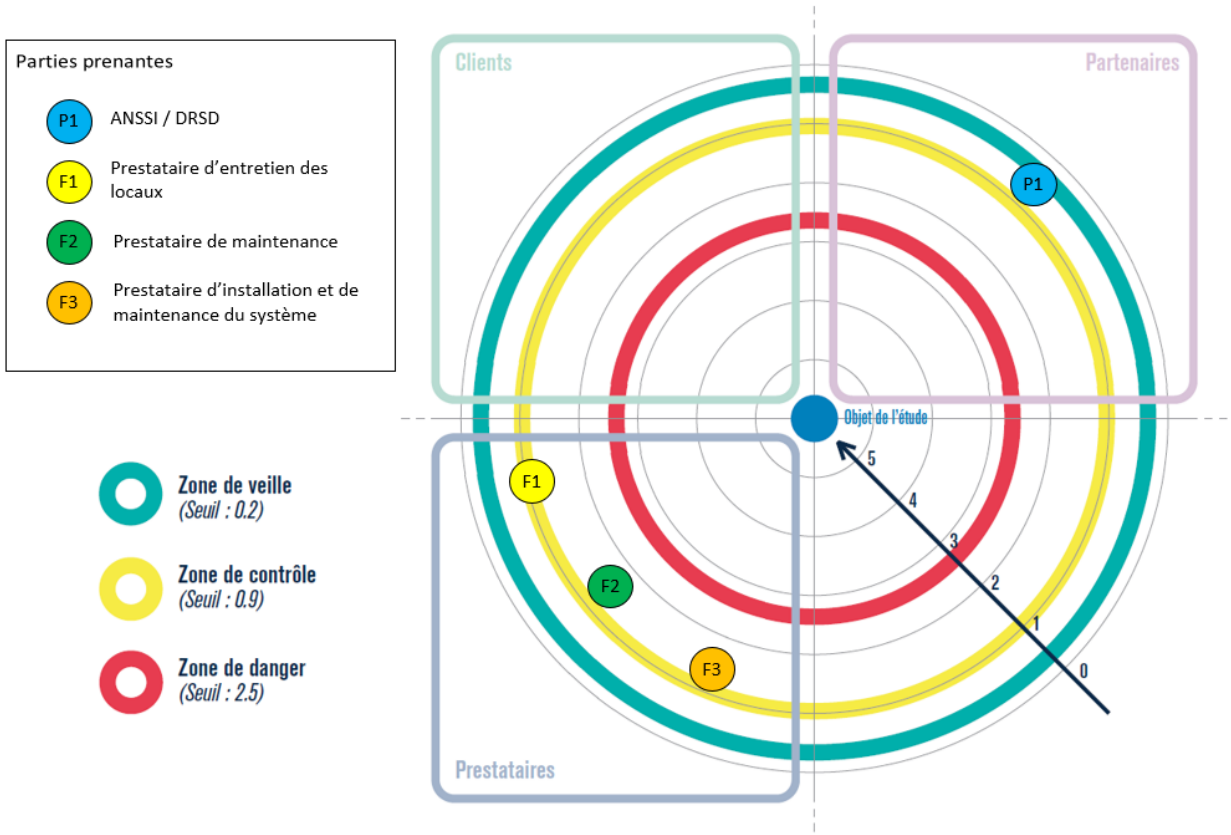

Figure 8 : Cartographie de la menace initiale de l'écosystème

La figure 8 permet de mettre en évidence les trois zones de menace que sont les zones de veille, de contrôle et la zone de danger ainsi que la position de chaque partie prenante vis-à-vis de ces zones [ANSSI - 2018b].

Pour les parties prenantes présentes dans la zone de veille (niveau de menace supérieur ou égal à 0.2 et inférieur à 0.9), la menace est considérée comme faible et peut être acceptée telle qu'elle. Ces parties prenantes ne seront pas prises en compte dans la construction des scénarios stratégiques.

Concernant la zone de contrôle, les parties prenantes s'y trouvant (niveau de menace supérieur ou égal à 0.9 et inférieur à 2.5) doivent faire l'objet d'une vigilance particulière et des mesures de sécurité pourront leurs être appliquées afin, si possible, de les faire rejoindre la zone de veille.

Enfin, la zone de danger contient les parties prenantes dont le niveau de menace est considéré comme très élevé (niveau de menace supérieur ou égal à 2.5) et qui ne doit pas être accepté dans l'état. Des mesures de sécurité doivent leurs être appliquées afin de faire baisser le niveau de menace.

2.5.2. Elaboration des scénarios stratégiques

L'élaboration des scénarios stratégiques permet de définir les chemins d'attaque que les sources de risque peuvent être susceptibles d'emprunter pour atteindre leurs objectifs visés. Ces chemins d'attaques peuvent être directs ou passer par l'écosystème, c'est-à-dire les parties prenantes identifiés dans la première partie de l'atelier. En fonction de l'objectif visé, il faudra bien entendu retenir uniquement les parties prenantes ayant un accès logique ou physique à la valeur métier visée.

Il est nécessaire d'établir un scénario stratégique pour chaque couple SR/OV retenu dans le tableau XVII page 39. Il s'agit de scénarios de haut niveau ne rentrant pas dans le détail technique de l'attaque. Ils doivent être construits par déduction et en se plaçant du point de vue de l'attaquant, en se demandant quelle valeur métier et donc quel bien support il doit viser pour atteindre son objectif mais également par quelle partie prenante l'accès à cette valeur métier peut être facilité.

Les scénarios stratégiques élaborés sont les suivants :

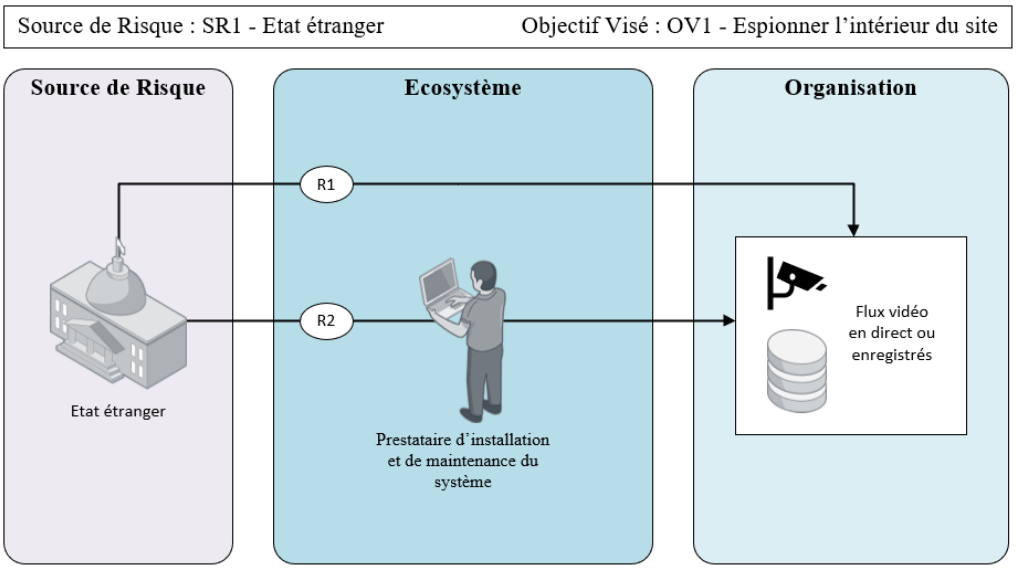

Figure 9 : Scénario stratégique n°1

Le scénario stratégique présenté en figure 9 se place du point de vue de l'état étranger dont l'objectif est d'espionner le site via le système de vidéoprotection.

Deux chemins d'attaques sont identifiés. Le premier, identifié R1, est un chemin d'attaque direct. Il sera probablement exécuté en établissant une connexion directe au réseau du système. Le second chemin d'attaque, identifié R2, passe par le prestataire d'installation et de maintenance du système de vidéoprotection. La source de risque utilisera probablement ici un moyen de corruption du prestataire pour atteindre son objectif.

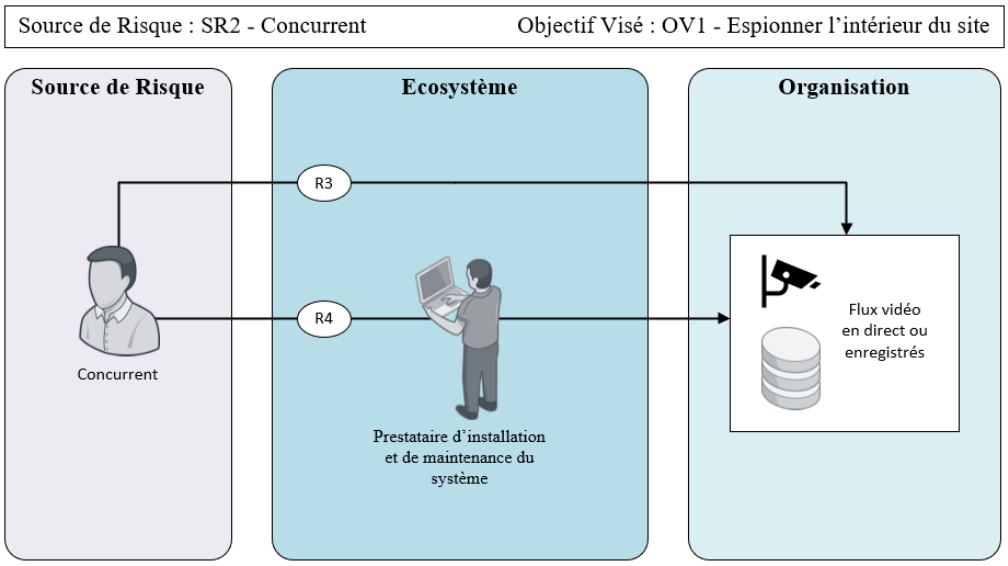

Figure 10 : Scénario stratégique n°2

Le scénario stratégique de la figure 10 se place du point de vue du concurrent dont l'objectif est également d'espionner le site via le système de vidéoprotection.

L'objectif visé du scénario étant le même, les deux chemins d'attaque R3 et R4 envisagés sont équivalents à ceux du scénario n°1 présenté en figure 9.

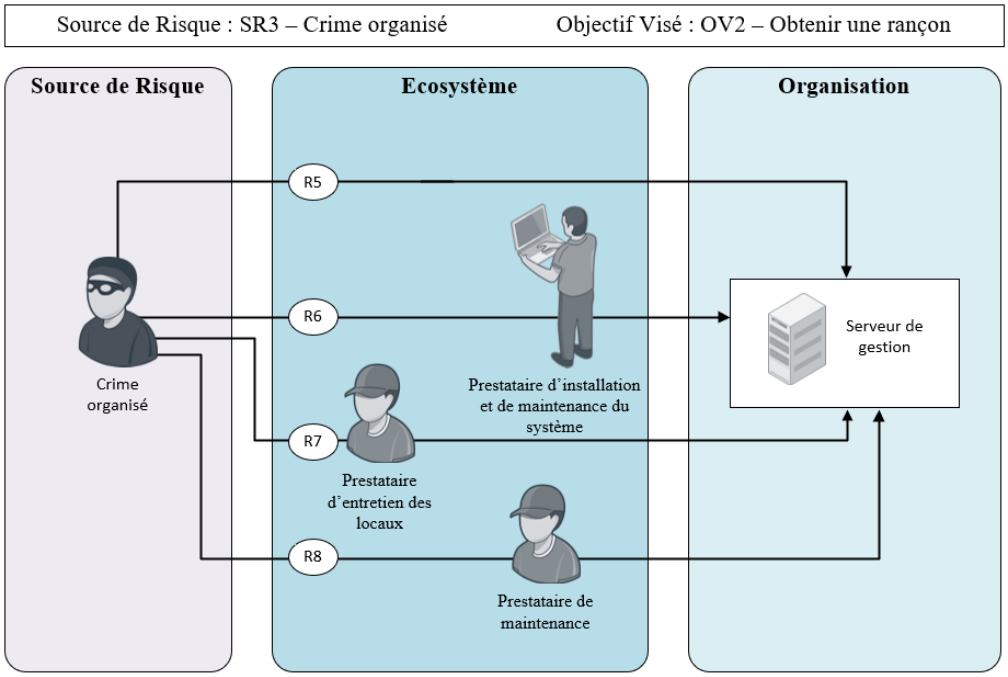

Figure 11 : Scénario stratégique n°3

Le scénario stratégique n°3 présenté en figure 11 se place du point de vue du crime organisé dont l'objectif serait d'obtenir une rançon de la part de l'organisation.

Quatre chemins d'attaque sont ici imaginés. Le premier, identifié R5, est l'équivalent du chemin d'attaque direct R1 identifié dans le scénario stratégique n°1. Le second, identifié R6, est également l'équivalent du chemin d'attaque R2 du scénario n°1, qui passe par le prestataire d'installation et de maintenance du système de vidéoprotection. Les deux chemins d'attaque suivants, identifiés R7 et R8, passent quant à eux par les deux autres parties prenantes identifiées précédemment que sont le prestataire d'entretien des locaux et le prestataire de maintenance. Ces parties prenantes ne disposent pas forcément d'accès logique au système mais ils disposent d'un accès physique aux locaux protégés et donc aux biens supports du système. Par exemple le personnel d'entretien sera susceptible d'accéder physiquement aux postes de visualisation du système et le prestataire de maintenance pourra certainement accéder aux locaux techniques hébergeant les actifs réseau et les serveurs de gestion. On peut également ici supposer que la corruption sera un moyen d'accès de la source de risque aux parties prenantes.

Les deux scénarios suivants, présentés dans les figures 12 et 13, se placent également du point de vue du crime organisé avec pour objectif de pénétrer sur le site pour commettre un vol pour le scénario stratégique n°4 et de rendre impossible les enregistrements pour le scénario stratégique n°5.

Bien que les biens supports visés ici soient différents, les chemins d'attaque sont équivalents à ceux identifiés dans le scénario stratégique numéro 3 :

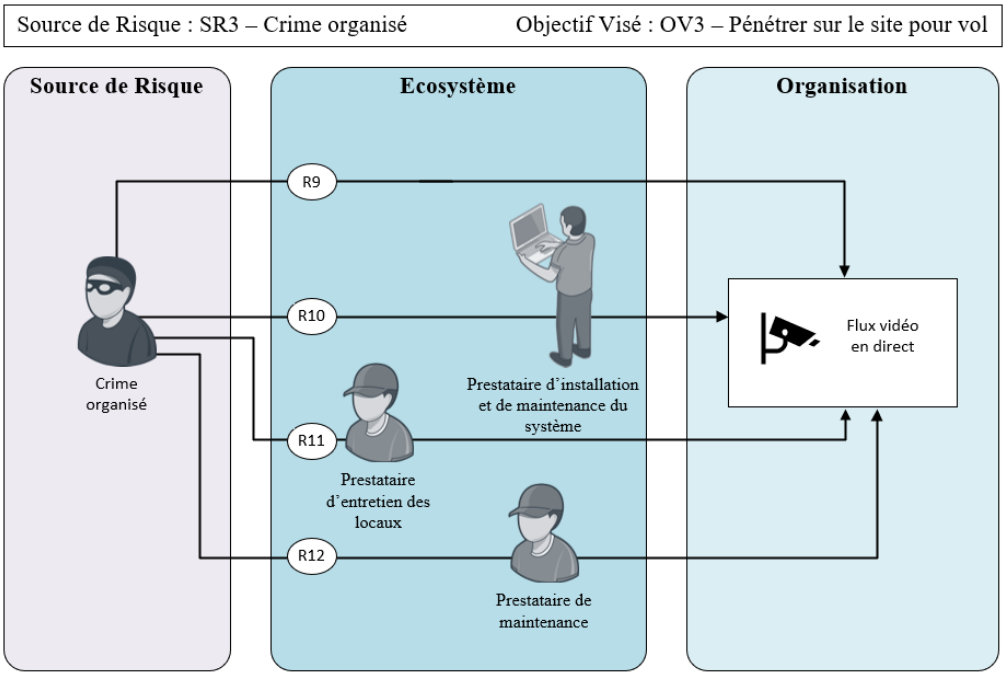

Figure 12 : Scénario stratégique n°4

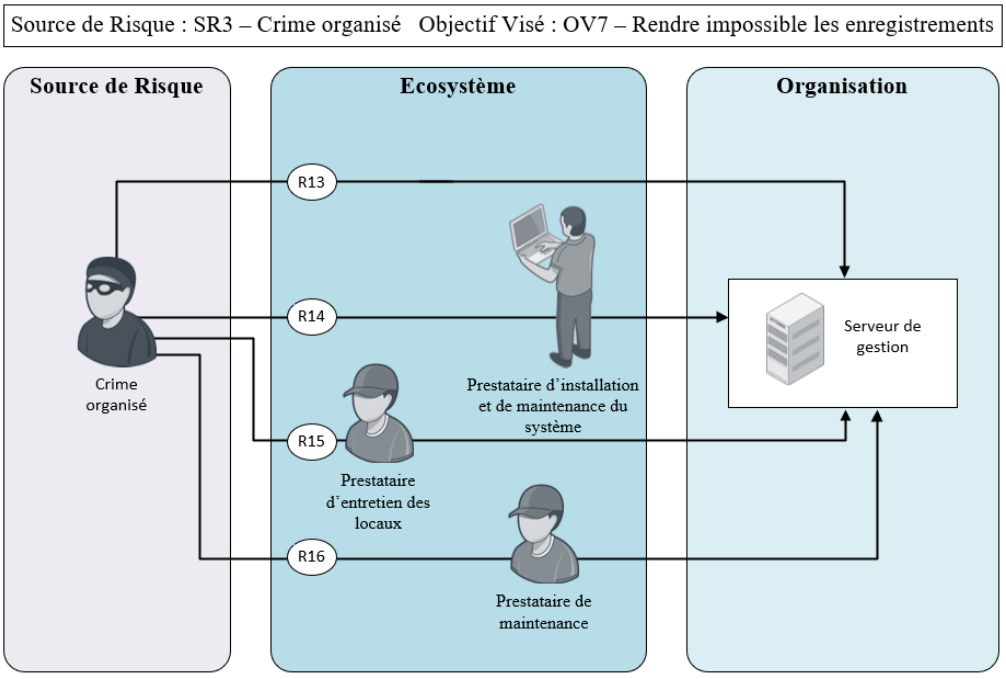

Figure 13 : Scénario stratégique n°5

Les scénarios stratégiques élaborés sont résumés dans le tableau suivant, leur gravité est reprise depuis le tableau XIII page 33 en lien avec les événements redoutés associés:

Tableau XXII : Liste des scénarios stratégiques et chemins d'attaques identifiés

Scénarios stratégiques identifiés				
Couple SR/OV		**Chemins d'attaques**		**Gravité**
Source de risque	**Objectif Visé**	**Id**	**Nom**	
SR1	OV1	R1	Accéder aux flux vidéo des caméras directement	4
		R2	Accéder aux flux vidéo des caméras via le prestataire d'installation du système	
SR2	OV1	R3	Accéder aux flux vidéo des caméras directement	4
		R4	Accéder aux flux vidéo des caméras via le prestataire d'installation du système	
SR3	OV2	R5	Rendre inopérant le serveur de gestion directement	4
		R6	Rendre inopérant le serveur de gestion via le prestataire d'installation du système	
		R7	Rendre inopérant le serveur de gestion via le prestataire d'entretient des locaux	
		R8	Rendre inopérant le serveur de gestion via le prestataire de maintenance du site	
SR3	OV3	R9	Rendre indisponible les flux vidéo des caméras directement	4
		R10	Rendre indisponible les flux vidéo des caméras via le prestataire d'installation du système	
		R11	Rendre indisponible les flux vidéo des caméras via le prestataire d'entretient des locaux	
		R12	Rendre indisponible les flux vidéo des caméras via le prestataire de maintenance du site	
SR3	OV7	R13	Rendre inopérant le serveur de gestion directement	4
		R14	Rendre inopérant le serveur de gestion via le prestataire d'installation du système	
		R15	Rendre inopérant le serveur de gestion via le prestataire d'entretient des locaux	
		R16	Rendre inopérant le serveur de gestion via le prestataire de maintenance du site	

2.5.3. Mesures de sécurité sur l'écosystème

L'élaboration des scénarios stratégiques a permis de mettre en évidence que les parties prenantes de l'écosystème peuvent présenter un vecteur d'attaque. Il est donc nécessaire de déterminer des mesures de sécurité applicables à ces parties prenantes afin de réduire leur niveau de menace.

Les différents choix pour l'organisation dans ce cas sont les suivants :

- Remplacer la partie prenante par une nouvelle répondant à certaines exigences permettant par exemple d'augmenter le niveau de maturité cyber
- Réduire le niveau de dépendance vis-à-vis de cette partie prenante
- Réduire le niveau de pénétration de la partie prenante et réduisant par exemple ses accès au système ou en ajoutant des contrôles spécifiques

Dans le cas de cette étude, on peut remarquer que le niveau de pénétration du prestataire d'entretien et du prestataire de maintenance pourrait être réduit en supprimant les accès physique aux locaux protégés ou en les autorisant uniquement en étant accompagné. Le niveau de maturité cyber de ces mêmes prestataires pourrait également être augmenté en réalisant des sessions de sensibilisation des collaborateurs œuvrant sur le site.

Le niveau de menace de certaines parties prenantes ne peut malheureusement pas être atténué, il conviendra alors de traiter le risque avec des mesures de sécurité supplémentaires appliquées sur le système.

Tableau XXIII : Mesures se sécurité applicables à l'écosystème

Mesures de sécurité applicables à l'écosystème		
Catégorie	**Nom**	**Mesure de sécurité**
Prestataire	F1 - Prestataire d'entretien des locaux	Interdire l'accès aux locaux protégés
Prestataire	F1 - Prestataire d'entretien des locaux	Réaliser des sessions de sensibilisation du prestataire aux risques cyber
Prestataire	F2 - Prestataire de maintenance	Autorisé l'accès aux locaux protégés uniquement en étant accompagné
Prestataire	F2 - Prestataire de maintenance	Réaliser des sessions de sensibilisation du prestataire aux risques cyber

2.5.4. Niveau de menace et cartographie résiduelle de l'écosystème

À la suite de l'application des mesures de sécurité définies précédemment, le niveau de menace des parties prenantes peut être réévalué :

Tableau XXIV : Evaluation résiduelle des parties prenantes

Evaluation résiduelle des parties prenantes						
Catégorie	**Nom**	**Dépendance**	**Pénétration**	**Maturité Cyber**	**Confiance**	**Niv. De Menace**
Partenaire	P1 - ANSSI/DRSD	4	3	4	4	**0,75**
Prestataire	F1 - Prestataire d'entretien des locaux	1	1	3	2	**0,16**
Prestataire	F2 - Prestataire de maintenance	2	2	3	2	**0,66**
Prestataire	F3 - Prestataire d'installation et de maintenance du système	3	4	3	3	**1,33**

Le niveau de menace de chaque partie prenante est ensuite représenté graphiquement sur la cartographie de la menace résiduelle :

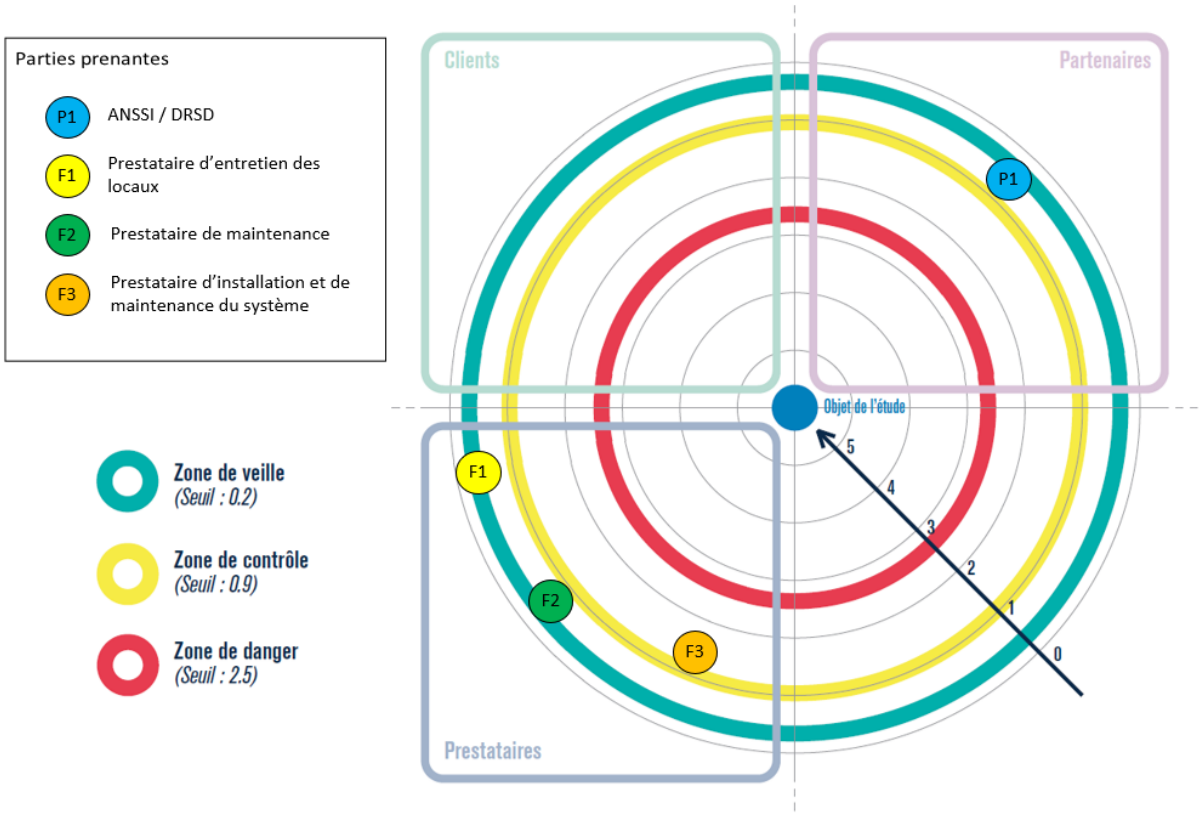

Figure 14 : Cartographie de la menace résiduelle de l'écosystème

2.6. Scénarios opérationnels

Bien que cette étude ne nécessite pas l'élaboration des scénarios opérationnels, ce paragraphe va tout de même expliquer la méthode de réalisation de ces derniers.

Le principe de cet atelier est qu'à chaque chemin d'attaque identifié dans l'atelier précédent correspond un scénario opérationnel, consistant en une suite d'actions élémentaires réalisées par l'attaquant pour atteindre son objectif.

Les données d'entrée de cet atelier sont donc les chemins d'attaque de l'atelier 3 ainsi que les différents éléments identifiés dans les deux premiers ateliers, et les données de sortie seront les scénarios opérationnels évalués selon leur vraisemblance.

2.6.1. Elaboration des scénarios opérationnels

Les scénarios opérationnels sont basés sur une séquence d'attaque type qui est composée des quatre phases suivantes :

- Connaitre : cette phase consiste à trouver et rassembler des informations qui seront utiles à l'attaque. Ces informations peuvent être de nature technique, comme la cartographie du système d'information cible, ou concerner l'écosystème, comme identifier les personnes ayant des accès privilégiés au SI. Cette phase de reconnaissance est réalisée par tous les moyens dont dispose la source de risque, comme par exemple l'exploitation des réseaux sociaux professionnels, les approches directs des collaborateurs de l'organisation ou le vols d'information résultant d'une précédente attaque.
- Rentrer : le deuxième phase du scénario consiste, pour la source de risque, à s'introduire dans le système d'information ciblé en attaquant les biens supports de ce dernier. Cette attaque est le plus souvent réalisée via l'exploitation des vulnérabilités techniques ou organisationnelles identifiés grâce à la phase « Connaitre ».
- Trouver : cette troisième phase se compose des actions élémentaires exécutées par la source de risque pour effectuer une reconnaissance interne du système d'information afin d'obtenir des privilèges supplémentaires, d'effectuer une latéralisation vers un autre système et mettre en place des portes dérobés qui lui permettront un accès au SI sur la durée.

- Exploiter : enfin, la quatrième et dernière phase consiste à utiliser les moyens mis en place dans la phase « Trouver » pour atteindre l'objectif visé, comme par exemple effectuer une exfiltration de données ou rendre un système inopérant.

Chaque action réalisée lors des ces différentes phase est nommée dans la méthode action élémentaire (AE). Pour la conception des scénarios opérationnels et notamment le choix des actions élémentaires, il est possible de se baser sur des bases de données qui recensent les méthodes et vulnérabilités connues.

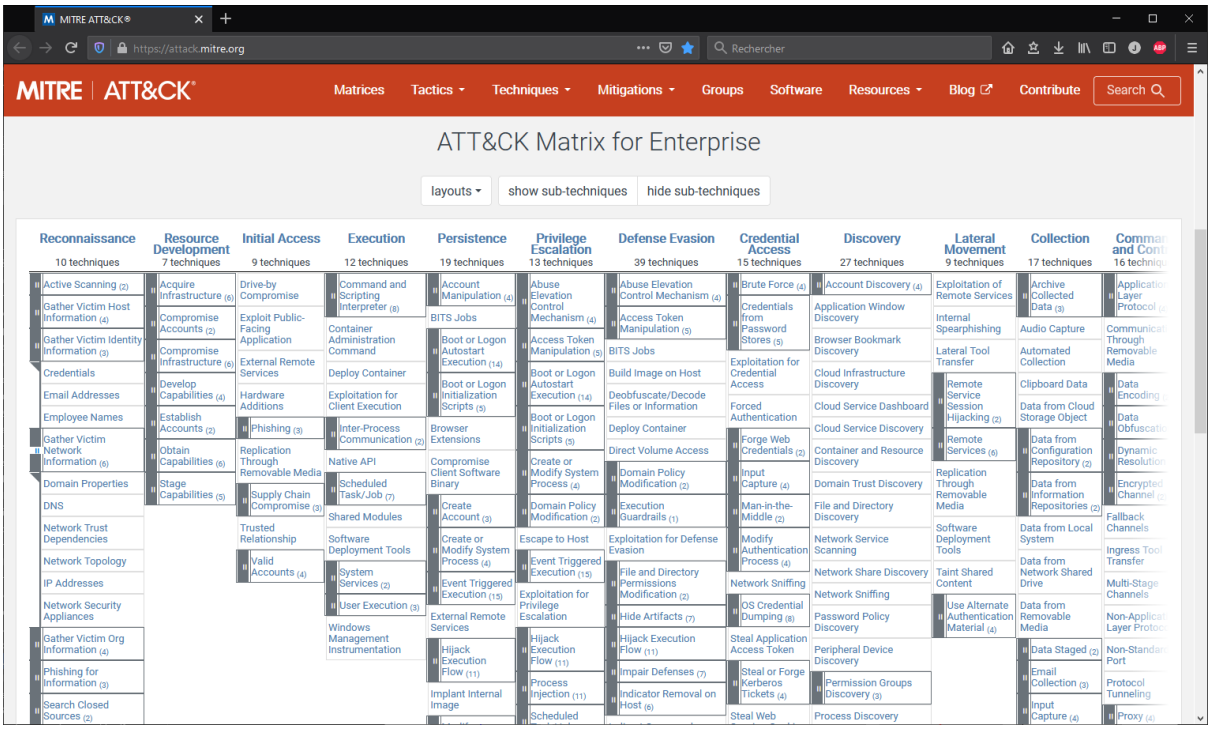

Figure 15 : Site Internet MITRE ATT&CK détaillant les techniques d'attaque et les vulnérabilités

La figure 15 est une capture d'écran du site internet MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) qui propose une base de connaissance regroupant divers types d'attaques et vulnérabilités utilisées par les sources de risques reconnues dans le monde de la cybersécurité.

Le Club EBIOS propose également un outil sous la forme d'un tableur Excel qui reprend et traduit la base de connaissance proposée par MITRE [CLUB EBIOS - 2021].

Il faudra également consulter les différents centres d'alertes, nommés Computer Emergency Response Team (CERT), qui recenses les vulnérabilités connues des logiciels et matériels ainsi que les menaces et incidents de cybersécurité qui sont en cours.

2.6.2. Evaluation de la vraisemblance

Chaque scénario opérationnel doit être évalué selon sa vraisemblance. Pour cela, la méthode propose trois approches d'évaluation :

- La méthode expresse : cette méthode propose une valorisation directe de la vraisemblance globale du scénario.
- La méthode standard : cette méthode se base sur la valorisation de la probabilité de succès de chaque action élémentaire du scénario. La vraisemblance globale du scénario sera alors égale à la vraisemblance la plus faible d'une des actions élémentaires.
- La méthode avancée : cette méthode consiste en la valorisation à la fois de la probabilité de succès de chaque action élémentaire mais également de sa difficulté technique. La vraisemblance globale du scénario sera alors égale à la vraisemblance la plus faible d'une des actions élémentaires.

Une échelle est alors nécessaire pour évaluer cette vraisemblance, voici celle proposée par la méthode [ANSSI - 2018b] qu'il sera possible d'adapter en fonction du besoin :

Tableau XXV : Echelle d'évaluation de la vraisemblance des scénarios opérationnels

Echelle	Description
V4 - Quasi certain	La source de risque va certainement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est très élevée.
V3 - Très vraisemblable	La source de risque va probablement atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est élevée.
V2 - Vraisemblable	La source de risque est susceptible d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est significative.
V1 - Peu vraisemblable	La source de risque a peu de chance d'atteindre son objectif visé selon l'un des modes opératoires envisagés. La vraisemblance du scénario est faible.

Dans le cas où la méthode avancée serait choisie, il sera nécessaire d'établir deux échelles supplémentaires :

- Une échelle de difficulté technique : celle-ci permettra d'évaluer la difficulté technique de réalisation d'une action élémentaire par la source de risque en termes de ressources à engager (temps et moyens financiers nécessaires), par exemple sur quatre niveaux de faible à très élevée en passant par modérée et élevée
- Une échelle de cotation globale : cette dernière, représentée sou forme de matrice, permettra de combiner les valeurs de vraisemblance et de difficulté technique pour attribuer une note globale à l'action élémentaire

2.6.3. Exemple de scénario opérationnel

L'exemple ci-dessous est basé sur le chemin d'attaque R8 identifié dans le scénario stratégique n°3 présenté en figure 11. Ce scénario se plaçait du point de vue du crime organisé dont l'objectif est d'obtenir une rançon de la part de l'organisation.

Pour la phase « Connaitre », la méthode de reconnaissance par source ouverte est privilégiée. En effet il est facilement possible, par une source de risque, de savoir quelle entreprise est chargée de la maintenance en observant par exemple les allées et venues des entreprises sur le site.

Pour la phase « Rentrer », la méthode consiste à corrompre un technicien de l'entreprise de maintenance afin qu'il introduise et connecte au système une clé USB infectée d'un rançongiciel.

La phase « Trouver » consiste quant à elle à la propagation du rançongiciel aux différents équipements du système par le réseau.

Enfin, la phase « Exploiter » mettra en place le chiffrement des données pour rendre le système inopérable et l'affichage d'un message d'information à destination de l'organisation lui expliquant comment effectuer le paiement de la rançon dans le but de le rendre disponible à nouveau.

La méthode standard est ensuite utilisée pour évaluer la vraisemblance de chaque action élémentaire du scénario et sa vraisemblance globale est ainsi retenue par rapport à la valeur la plus faible identifiée sur les actions élémentaires. La gravité du scénario correspond quant à elle à la gravité de l'événement redouté associé.

Enfin, le scénario opérationnel élaboré est représenté sous forme graphique, comme le propose la méthode EBIOS RM :

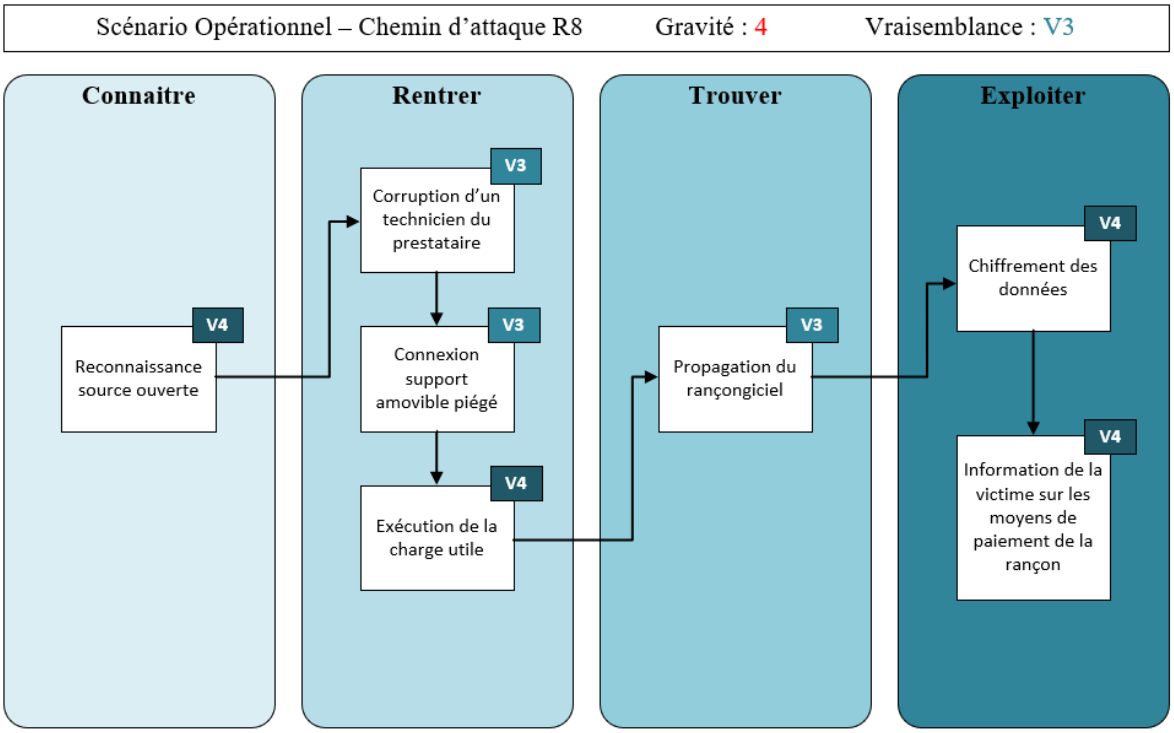

Figure 16 : Scénario Opérationnel correspondant au chemin d'attaque R8

2.7. Traitement du risque

D'après la norme ISO 27005 qui traite de la mise en place de la sécurité de l'information par une approche de gestion du risque, chaque risque identifié peut être :

- Réduit : la mise en place de mesures de sécurité complémentaires au socle de sécurité permet de réduire certaines propriétés du risque, comme sa vraisemblance ou sa gravité
- Maintenu : le risque est accepté dans l'état sans mesure de sécurité additionnelle
- Refusé : le risque est refusé, il faut alors trouver les mesures adapté pour supprimer complètement le risque
- Partagé : le risque est transféré à un tier, par exemple par la souscription de contrat d'assurance

Il appartient alors à l'organisation de définir le Plan d'Amélioration Continue de la Sécurité (PACS). Ce processus vise à recenser les mesures de sécurité, identifiées tout au long de l'analyse de risque, qui devront être mises en œuvre tout en évaluant leurs coût et leurs complexité et en leurs affectant une niveau de priorité.

Dans le cas de l'objet de l'étude, il convient en premier lieu de se concentrer sur l'application des mesures de sécurité identifiées dans le socle de sécurité et listées dans les tableaux IX et X page 29 et XI page 30, mais également celles concernant les parties prenantes mises en évidence dans l'atelier d'élaboration des scénarios stratégiques et listées dans le tableau XXIII page 50.

A la prochaine itération du cycle opérationnel, qui pourra être réalisée une fois le système installé, l'élaboration des scénarios opérationnels permettront sûrement de mettre en lumière de nouveaux risques qu'il faudra alors traiter par de nouvelles mesures.

3. Sécurisation du réseau

La seconde étape du projet étant de proposer une solution technique permettant de sécuriser le réseau d'un système d'information dédié à la vidéoprotection, seules les mesures de sécurité identifiées dans l'analyse de risque et s'appliquant au réseau du système seront étudiées.

Ces mesures, extraites de celles listées dans les tableaux IX et X page 29 et XI page 30, sont les suivantes. Elle se rapportent pour la plupart au principe de cloisonnement du réseau ainsi qu'à la mise en place d'un mécanisme de contrôle d'accès réseau :

Tableau XXVI : Liste des mesures de sécurité applicables au réseau

Référentiel source	Mesure de sécurité
Réf 1	Segmenter le réseau et mettre en place un cloisonnement entre ces zones
Réf 1	Utiliser un réseau dédié et cloisonné pour l'administration du système d'information
Réf 2	Cloisonner physiquement ou logiquement les SI
Réf 2	Privilégier une connectivité filaire pour les dispositifs de vidéoprotection
Réf 2	Cloisonner logiquement par type les dispositifs au sein du réseau support
Réf 2	Désactiver les ports inutilisés sur les commutateurs réseau
Réf 2	Contrôler les accès aux ports réseau par authentification ou à minima par vérification des adresses MAC
Réf 2	Cloisonner logiquement le réseau des caméras extérieures
Réf 2	Filtrer les flux entre les réseaux
Réf 2	Chiffrer et authentifier les flux émis et reçus par les caméras
Réf 3	Désactiver les protocoles obsolètes (telnet, ftp…)

3.1. Plateforme de test

La plateforme de test est constituée des matériels et logiciels généralement mis en œuvre dans les systèmes de vidéoprotection installés par Securitas Sécurité Electronique. Elle contient donc :

- Un serveur de gestion de marque DELL et de type Poweredge sur lequel est installé le VMS Milestone XProtect
- Plusieurs caméras IP de marque Axis et de types Q1941-E et Q6215-LE
- Plusieurs commutateurs de marque Allied Telesis et de types AT-IE340-12GP-80 et AT-X530L-28GTX-50
- Un poste de visualisation de marque DELL et de type Optiplex sur lequel est installé le logiciel XProtect Smart Client

3.2. Cloisonnement du réseau

Le cloisonnement du réseau est une mesure de sécurité qui consiste à diviser le réseau support du système de vidéoprotection en plusieurs sous-réseaux. Ce cloisonnement peut être physique, c'est à dire réaliser plusieurs réseaux ayant chacun leurs propres équipements actifs (commutateurs), où logique, c'est à dire réaliser le cloisonnement grâce à des protocoles spécifiques disponibles sur les commutateurs.

Pour des raisons économiques il n'est pas envisageable de cloisonner le réseau physiquement. En effet cela impliquerait des coûts supplémentaires car cela nécessiterait l'acquisition de commutateurs et la réalisation de liaisons réseaux additionnels.

Le cloisonnement logique du réseau est réalisable car ils nécessitent uniquement de la configuration supplémentaire sur les actifs réseaux déjà disponibles. Ce cloisonnement est possible via la création de réseaux locaux virtuels, appelés Virtual Local Area Network (VLAN), décrits par la norme IEEE 802.1Q.

3.2.1. Fonctionnement des VLAN

Les VLAN permettent donc de créer plusieurs sous-réseaux virtuels à l'intérieur d'un même réseau physique. Les données envoyées par un équipement appartenant à un VLAN ne seront pas visibles par les équipements appartenant aux autres VLAN.

Pour que les commutateurs puissent reconnaître à quel VLAN appartiennent les données qui circulent sur le réseau, ils ajoutent une étiquette à chaque trame Ethernet envoyée par l'équipement connecté au port [Lohier et Présent - 2020].

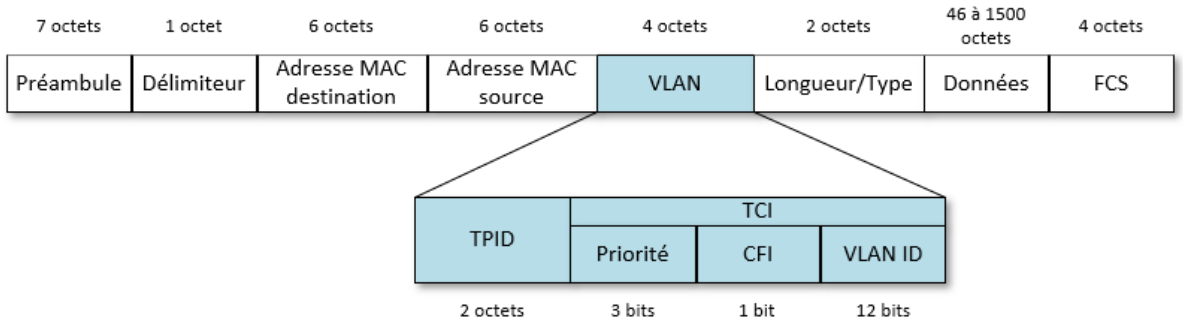

Figure 17 : Trame Ethernet avec étiquette VLAN

La figure 17 représente une trame Ethernet dans laquelle a été insérée par le commutateur une étiquette VLAN. Cette étiquette, d'une taille totale de quatre octets est placée immédiatement après l'adresse MAC source dans la trame et elle contient :

- TPID : Tag Protocol Identifier, sur deux octets, indique que l'étiquette est une étiquette de type VLAN, dans ce cas sa valeur en hexadécimale est fixée à 0x8100
- Priorité : sur trois bits permettant d'indiquer huit niveaux, indique la priorité de la trame, où la valeur 0 est la plus haute priorité
- CFI : Canonical Format Indicator, sur 1 bits, qui permet d'indiquer sir les données de la trame sont des données Ethernet, dans ce cas sa valeur sera 0
- VLAN ID : sur 12 bits, représente l'identifiant du VLAN, qui va de la valeur 1 à 4094, correspondant aux nombre de VLAN possibles sur un même réseau physique

Il existe plusieurs méthodes pour attribuer un identifiant de VLAN à chaque port d'un commutateur :

- Attribution statique : chaque port est configuré dans le commutateur pour correspondre à un identifiant de VLAN unique
- Attribution dynamique : une table de correspondance entre l'adresse MAC source des équipements et l'identifiant de VLAN est configurée dans les commutateurs, l'identifiant de VLAN est ainsi attribué au port dynamiquement en fonction de l'équipement qui est connecté dessus

Chaque port des commutateurs, en plus de l'identifiant de VLAN, doit être configuré dans un des modes suivant [Allied – 2021a] :

- Access : les ports en mode Access ne contiennent qu'un seul identifiant de VLAN, l'équipement raccordé sur ce port appartiendra donc au VLAN défini dans la configuration du port. Ces ports sont dits « Untagged », car les trames ethernet en provenance de l'équipement raccordé ne contiennent pas d'étiquette de VLAN, c'est le commutateur qui sera donc en charge de l'ajouter.
- Trunk : les ports en mode Trunk contiennent un ou plusieurs identifiants de VLAN, ils sont généralement utilisés pour réaliser les liaisons entre commutateurs qui nécessitent de faire circuler les données d'un ou plusieurs VLAN différents. Ces ports sont quant à eux dit « Tagged », car les trames ethernet en provenance des autres ports et devant transiter par les ports Trunk contiennent déjà l'étiquette du VLAN.

La configuration des différents ports, en fonction des éléments cités précédemment et de leurs finalités, sera donc :

- Les ports sur lesquels sont raccordés un seul équipement (caméra IP, serveur de gestion, poste de visualisation) seront configurés en mode Access Untagged et associés à un seul identifiant de VLAN.
- Les ports servant de liaison entre les commutateurs seront quant à eux configurés en mode Trunk Tagged et associés aux différents identifiants de VLAN qu'ils devront faire transiter.

3.2.2. Mesures de sécurité complémentaires des commutateurs

Les réseaux virtuels ne sont pas exempts de vulnérabilités. En effet la conception de la norme sur lesquels ils reposent est basée au départ sur des besoins de segmentation des réseaux pour limiter les domaines de diffusion et ainsi réduire les phénomènes de congestion sur les réseaux de grande envergure, pas pour des besoins de sécurité [Allied – 2021a]. Il est donc primordial dans la configuration des commutateurs d'activer certaines options pour se prémunir de ces failles de sécurité.

Une des vulnérabilités induite par la configuration par défaut des commutateurs est la technique du saut de VLAN ou VLAN hopping [Llorens et al. - 2010]. En effet les ports du

commutateur, dans leur configuration par défaut, peuvent basculer automatiquement du mode Access au mode Trunk si un attaquant réussi à envoyer sur le port des paquets Ethernet dans un certain format. De plus s'il réussi à réaliser cette attaque sur un port se situant sur le VLAN par défaut du commutateur, il aura accès aux informations que les commutateurs s'échangent entre eux pour le fonctionnement global du réseau [ANSSI - 2016].

Pour se prémunir de cette vulnérabilité, il est indispensable de désactiver les ports inutilisés mais également, pour se protéger en cas de réactivation accidentelle, de les configurer sur un VLAN isolé dit de « quarantaine » ne servant qu'à accueillir ce type de port et de les forcer en mode Access [ANSSI - 2016].

3.2.3. Routage et filtrage des flux réseaux

Le réseau étant cloisonné en plusieurs réseaux virtuels, et les équipements connectés à ces réseaux nécessitant pour certains de communiquer entre eux, il sera nécessaire de mettre en place une solution de routage entre les VLAN. Le routage des flux pourrait simplement être effectué par les commutateurs eux-mêmes, mais ceux-ci ne sont pas conçus pour faire du routage de paquets au niveau 3 [ANSSI - 2016].

Il est donc indispensable de confier cette mission de routage à un routeur dédié qui permettra de n'autoriser les communications qu'entre certains équipements du réseau. Cette étape sera alors l'occasion de mettre en place une des mesures de sécurité préconisées qui est le filtrage des flux réseaux. Ces deux fonctionnalités seront assurées par le même équipement, le routeur firewall.

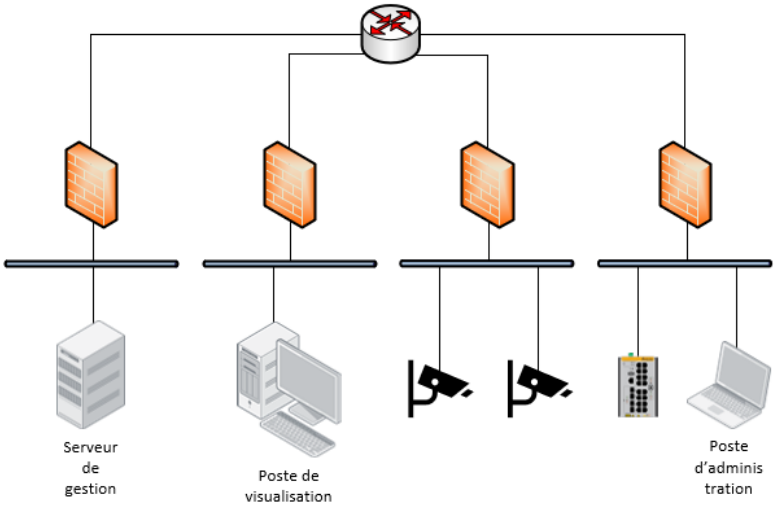

Figure 18 : Interconnexions des réseaux logiques et filtrage des flux

La figure 18 représente l'interconnexion des VLAN au travers du routeur firewall. Il s'agit de permettre aux équipements raccordés sur un VLAN de pouvoir communiquer avec des équipements d'autres VLAN grâce au routeur, tout en mettant des restrictions sur les flux transitant par le firewall. Chaque VLAN se retrouve alors connecté à un port réseau du routeur firewall, qui est configuré pour ne router qu'une partie des flux de certains équipements.

Pour effectuer cette configuration il faut définir la matrice des flux en recensant tous les flux réseaux nécessaires au bon fonctionnement du système. Ils sont identifiés par leurs sources et leurs destinations (caméra IP, serveur de gestion…) ainsi que par leurs appartenance aux différents VLAN. Il faut également préciser les ports TCP ou UDP qu'ils utilisent. Ces informations sont extraites du guide d'administration du logiciel Milestone XProtect [MILESTONE - 2021] :

Tableau XXVII : Matrice des flux réseaux

Source	VLAN Source	Destination	VLAN Dest.	Ports	Description
Caméras IP	40	Serveur de gestion	20	TCP 80 TCP 443 TCP 554	Flux vidéo des caméras
Serveur de gestion	20	Caméras IP	40	UDP 123	Flux NTP pour la synchronisation du temps
Serveur de gestion	20	Poste de visualisation	30	TCP 80 TCP 443 TCP 8081 TCP 8082	Flux de connexion du logiciel client au VMS
Poste d'administration	10	Caméras IP	40	TCP 80 TCP 443	Flux pour paramétrage à distance des caméras IP
Poste d'administration	10	Serveur de gestion	20	TCP 3389	Flux RDP pour administration à distance du serveur de gestion
Poste d'administration	10	Poste de visualisation	30	TCP 3389	Flux RDP pour administration à distance du poste de visualisation
Commutateurs	10	Serveur RADIUS	20	UDP 1812 UDP 1813	Flux servant à l'authentification RADIUS

3.2.4. Mise en œuvre sur la plateforme de test

L'ANSSI préconise de cloisonner le réseau par type d'équipement [ANSSI - 2020a] . Dans le système d'information de vidéoprotection, quatre type d'équipements sont à distinguer. Il y a tout d'abord les commutateurs qui constituent le réseau, les caméras IP, les postes de visualisation et enfin les serveurs de gestion. Le choix des VLAN à mettre en place est donc le suivant :

- VLAN n°10 : ce VLAN sera dédié à l'administration du réseau. Il contiendra les interfaces réseau des commutateurs pour permettre leurs configuration distante
- VLAN n°20 : ce VLAN permettra de cloisonner le ou les serveurs de gestion du système
- VLAN n°30 : ce VLAN contiendra exclusivement les postes de visualisation utilisés par les opérateurs du système
- VLAN n°40 : ce VLAN sera quant à lui dédié à la partie terrain du système, c'est-à-dire les caméras IP
- VLAN n°2000 : ce VLAN constitue le VLAN de quarantaine qui sera attribué aux ports inutilisés

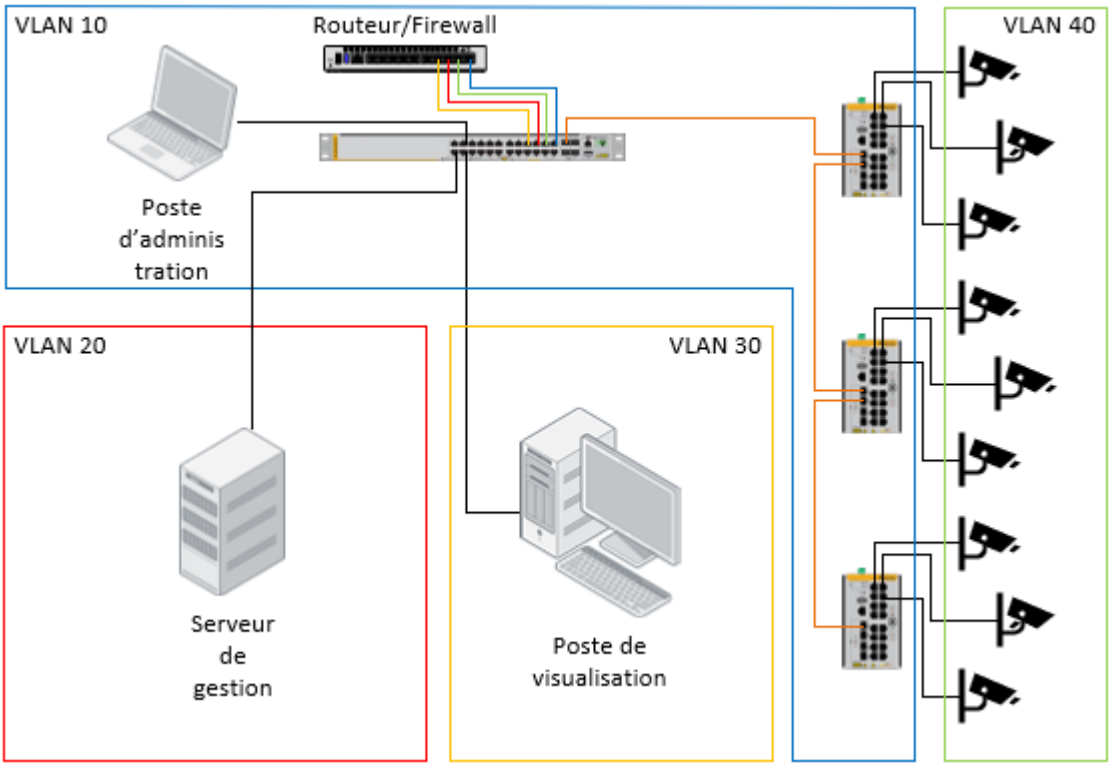

Figure 19 : Cloisonnement logique du réseau

La figure 19 représente le cloisonnement du réseau du système de vidéoprotection. Les numéros des quatre VLAN sont indiqués. Comme le préconise l'ANSSI [ANSSI - 2020a] , un poste dédié à l'administration du réseau est ajouté, il sera connecté sur un port configuré pour appartenir au VLAN n°10.

Pour l'attribution des numéros de VLAN aux ports des commutateurs, celle-ci sera faite de manière statique. En effet les équipements raccordés sur les commutateurs sont fixes, les caméras IP, serveurs de gestion et postes de visualisation seront toujours raccordés sur les mêmes prises réseaux.

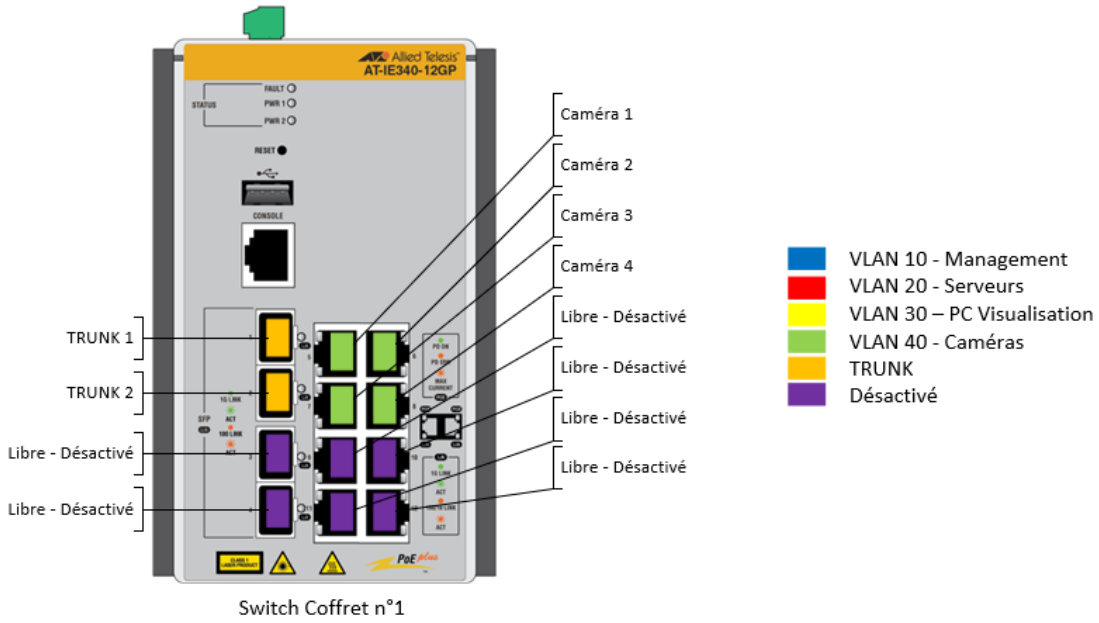

Figure 20 - Exemple de configuration des ports d'un commutateur

La figure 20 représente un exemple de configuration effectuée sur un commutateur. Les ports sur lesquels sont connectés les caméras sont configurés en mode Access Untagged avec attribution du VLAN n°40. Les ports servant à établir la liaison avec les autres commutateurs sont quant à eux configurés en mode Trunk Tagged avec attribution des VLAN n°10 et n°40. En effet ces ports doivent permettre de faire transiter les flux des caméras IP mais également les flux de management des commutateurs.

3.2.4.1. Configuration des commutateurs

Pour réaliser la configuration des VLAN dans les commutateurs, il sera nécessaire de suivre les étapes suivantes [Allied - 2021a] :

1) Se connecter à l'interface d'administration du commutateur.
2) Taper la commande « `enable` » afin d'activer la console.
3) Taper la commande « `configure terminal` » pour entrer en mode configuration.

Ces trois premières commandes sont à exécuter à chaque connexion au commutateur pour entrer en mode configuration.

4) Taper la commande « `vlan database` » pour modifier la base de données des VLAN créés dans le commutateurs.
5) Taper la commande « `vlan 10,20,30,40,2000` » pour créer les différents VLAN nécessaires.

Ensuite, pour chaque port sur lequel sera raccordé un équipement, il faudra exécuter les commandes suivantes :

1) Taper la commande « `interface port1.0.xx` » en remplaçant xx par le numéro du port à configurer.
2) Taper la commande « `switchport access vlan xx` » en remplaçant xx par l'identifiant du VLAN pour configurer le port en mode Access Untagged sur le VLAN souhaité.

Enfin, pour chaque port servant de liaison entre les commutateurs, il faudra exécuter les commandes suivantes :

1) Taper la commande « `interface port1.0.xx` » en remplaçant xx par le numéro du port à configurer.
2) Taper la commande « `switchport mode trunk` » pour définir le port en mode Trunk Tagged.
3) Taper la commande « `switchport trunk allowed vlan add xx,yy,zz` » en remplaçant xx, yy et zz par les identifiants des VLAN à attribuer au port.

Pour finir, afin de désactiver les ports non utilisés du commutateur comme préconisé, il faudra exécuter les commandes suivantes :

1) Taper la commande « `interface port1.0.xx` » en remplaçant xx par le numéro du port à désactiver
2) Taper la commande « `switchport access vlan 2000` » pour placer le port sur le VLAN isolé en mode Access
3) Taper la commande « `shutdown` » pour désactiver le port

3.2.4.2. Configuration du routeur firewall

Quatre ports physiques seront nécessaires pour interconnecter les VLAN entre eux au travers du routeur firewall. Chaque port du commutateur devra être configuré en mode Access sur chacun des VLAN :

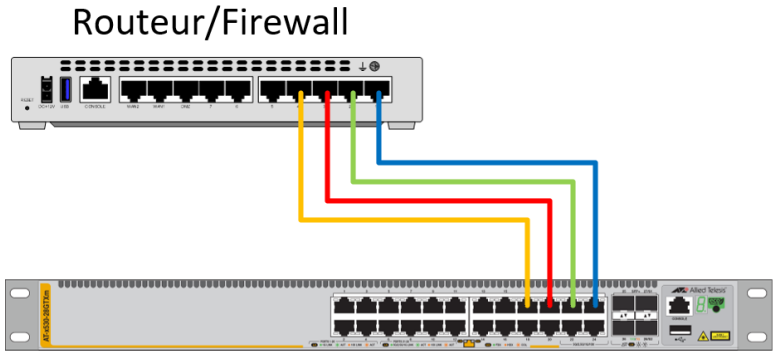

Figure 21: Connexions du routeur firewall au commutateur

La configuration du routeur firewall, afin de permettre le filtrage et le routage des flux des équipements, se réalise quant à elle directement depuis l'interface web de ce dernier [FORTINET - 2021]. Les points à configurer sont les suivants :

- Interfaces : il s'agit ici d'attribuer une adresse IP à chaque port physique du routeur firewall qui sera raccordé sur chacun des VLAN via plusieurs ports du commutateur. Ces adresses IP seront ensuite définies comme passerelle dans la configuration IP des équipements en fonction de leurs appartenances aux VLAN.

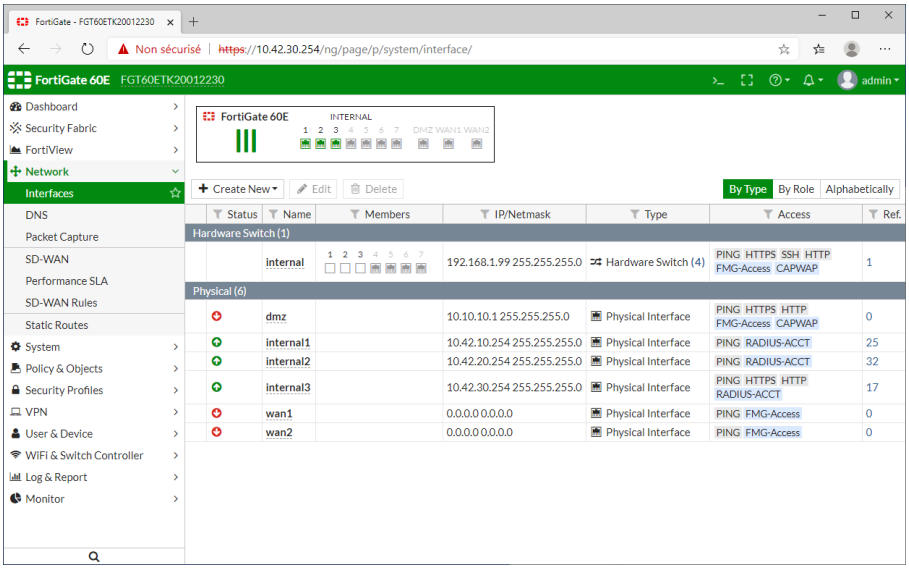

Figure 22 : Page de configuration des Interfaces du routeur firewall

- Addresses : il est ensuite nécessaire de créer dans le routeur firewall tous les équipements qui devront communiquer entre les VLAN. Il faut donc renseigner ici les adresses IP ou plages d'adresses IP de toutes les caméras, tous les serveurs de gestion, poste de visualisation et commutateurs utilisés.

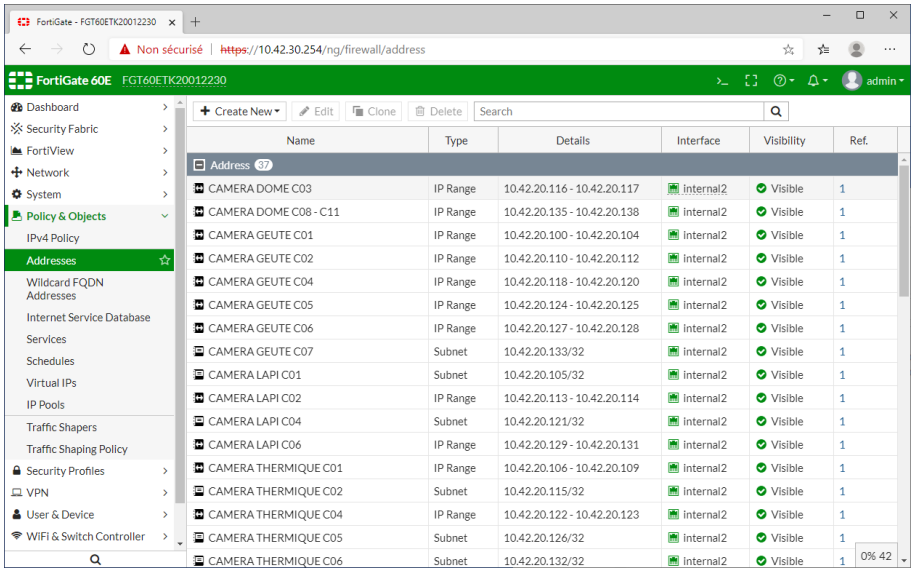

Figure 23 : Page de configuration des Addresses du routeur firewall

- Services : c'est dans ce point qu'il faut renseigner les ports réseau utilisés par les différents équipements. Ces ports sont listés dans la matrice des flux élaborée précédemment dans le tableau XXVII page 63.

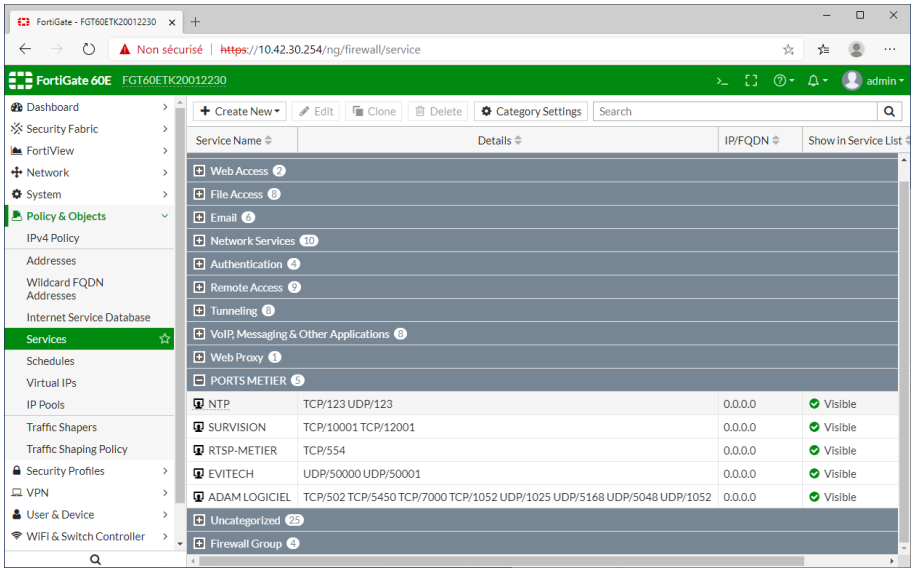

Figure 24 : Page de configuration des Services du routeur firewall

- IPv4 Policy : Enfin, c'est ici qu'il faut créer les règles de routage telles que définies plus tôt dans la matrice des flux réseaux du tableau XXVII page 63. Il faut associer les objets sources avec les objets destinations en utilisant les services, et donc les ports réseaux, dont ils ont besoin pour communiquer entre eux.

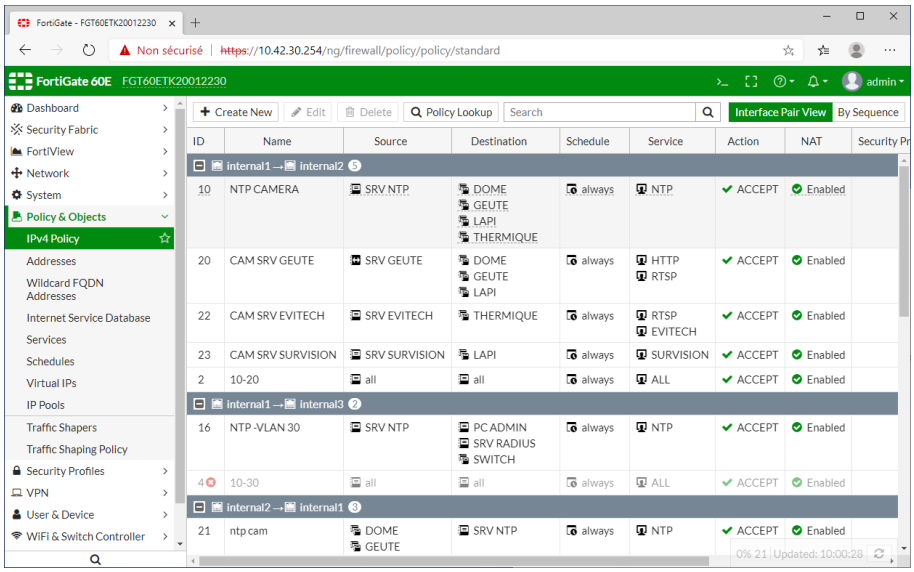

Figure 25 : Page de configuration des IPv4 Policy du routeur firewall

3.3. Contrôle d'accès réseau

Le principe de contrôle d'accès réseau est une mesure de sécurité qui permet de s'assurer que les périphériques qui accèdent au réseau sont bien autorisés à s'y connecter.

Ce contrôle d'accès est possible au niveau local des commutateurs, en utilisant par exemple le principe de filtrage des équipements par leurs adresses MAC, mais les recommandations de l'ANSSI se portent sur une méthode de contrôle d'accès centralisée par authentification [ANSSI - 2020a], généralement mise en œuvre via l'utilisation du protocole RADIUS, décrit par la norme IEEE 802.1x.

3.3.1. Fonctionnement du protocole RADIUS

Le protocole RADIUS est basé sur le modèle Authentication, Authorization et Accounting (AAA) [Bordères - 2006] :

- Authentication : permettre d'authentifier le client et de s'assurer ainsi de son identité
- Authorization : permettre d'accorder des droits d'accès au client sur le réseau
- Accounting : enregistrer la traçabilité d'accès au réseau du client, c'est-à-dire garantir la non-répudiation de ses accès

Trois éléments sont nécessaires au fonctionnement du contrôle d'accès réseau utilisant le protocole RADIUS :

- Le supplicant : il s'agit de l'équipement qui souhaite se connecter au réseau. Cet équipement doit être compatible avec la norme IEEE 802.1x. Dans le cas du système de vidéoprotection les clients sont les caméras IP.
- L'authentificateur : également appelé Network Access Server (NAS) ou client, ce sont les équipements qui vont avoir la charge de fournir l'accès réseau aux clients, en l'occurrence les commutateurs. Ces équipements doivent également être compatibles avec la norme IEEE 802.1x.
- Le serveur d'authentification : également nommé « Authentication server », c'est l'équipement qui a la charge d'authentifier les clients et ainsi autoriser ou non l'authentificateur à leurs donner l'accès au réseau. Dans le cas du système du vidéoprotection ce rôle est joué par le serveur RADIUS.

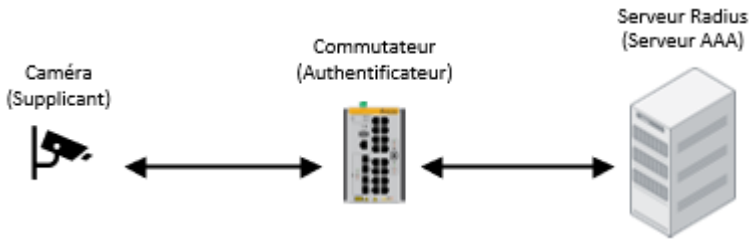

Figure 26 : Equipements s'impliquant dans le contrôle d'accès réseau

La figure 26 représente les équipements s'impliquant dans le processus de contrôle d'accès réseau via le protocole RADIUS ainsi que les directions des échanges de paquets qui s'effectuent entre eux. Les supplicants (Caméras IP) ne communiquent jamais directement avec le serveur RADIUS. Ce sont les authentificateurs (commutateurs) qui sont en charge de faire l'intermédiaire entre ces deux équipements.

Les ports des commutateurs configurés pour utiliser l'authentification RADIUS peuvent se trouver dans deux états :

- Non autorisé : c'est l'état par défaut du port. L'accès au réseau n'est alors pas possible pour un équipement connecté. Seul les trames EAP permettant de faire circuler les informations d'authentification sont autorisées entre le commutateur et l'équipement connecté.
- Autorisé : c'est l'état du port après une authentification réussi de l'équipement connecté. Dans cet état le port accepte tous les types de trame et permet donc les communications de l'équipement sur le réseau.

Les trames échangés entre les commutateurs et le serveur RADIUS peuvent être de quatre types :

- Access-Request : il s'agit du premier type de trames envoyées par le commutateur au serveur RADIUS à la connexion du supplicant. Cet échange contient plusieurs attributs tels que les champs « User-Name » configuré dans le supplicant ainsi que le « Calling-Station-Id » qui correspond à son adresse MAC.
- Access-Challenge : ce type de trame est ensuite envoyé par le serveur RADIUS au commutateur. Il s'agit pour le serveur d'authentification de demander l'envoi d'informations supplémentaires qui lui permettrons d'authentifier le supplicant, comme l'envoi d'un couple identifiant/mot de passe ou l'échange de certificats.

- Access-Accept : si l'authentification du supplicant est réussie par le serveur RADIUS, il enverra ce type de trame au commutateur pour qu'il autorise au supplicant l'accès au réseau en faisant basculer le port en mode autorisé.
- Access-Reject : au cas où l'authentification du supplicant par le serveur RADIUS échoue, il enverra alors de type de trame au commutateur qui refusera alors au supplicant l'accès au réseau en laissant le port en mode non autorisé.

La séquence de ces échanges et types de trames envoyées entre les différents équipements est la suivante :

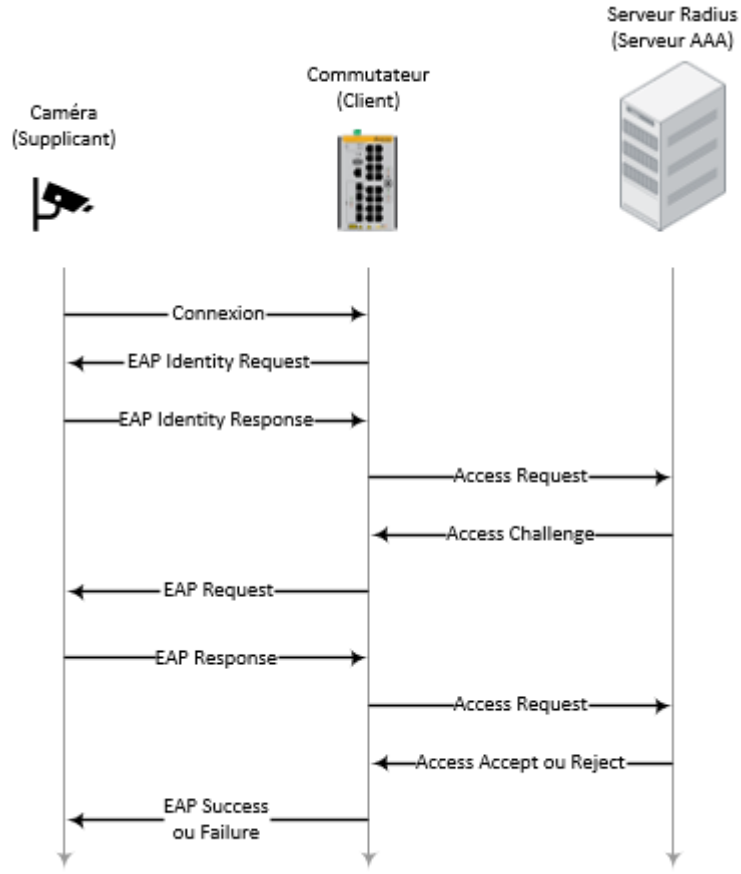

Figure 27: Séquence des échanges entre supplicant, client et serveur d'authentification

Le serveur RADIUS permet l'utilisation de plusieurs méthodes d'authentification dont les plus utilisées sont les suivantes [Bordères - 2006] :

- EAP-MD5 : l'authentification EAP-MD5 repose sur l'utilisation d'un couple identifiant/mot de passe, ce mode est réputé peu sécurisé du fait de l'obsolescence de la fonction de hachage MD5 [ANSSI - 2018c].

- EAP-TLS : cette méthode consiste à la mise en place d'un processus d'échange de certificats entre le serveur d'authentification et le client. Ceci permet une authentification mutuelle des équipements, le client s'assurant d'abord de l'identité du serveur avant de lui délivrer sa propre identité. Pour cela il est nécessaire d'utiliser plusieurs certificats, un pour le serveur d'authentification et autant de certificats qu'il y a de clients. Ce protocole est considéré comme sûr par l'ANSSI [ANSSI - 2018c].
- EAP-PEAP : souvent nommé uniquement PEAP, cette méthode d'authentification repose sur deux phases. Dans un premier temps, le serveur d'authentification s'authentifie lui-même auprès du client afin de mettre en place un tunnel TLS qui permettra de sécuriser les communications entre eux. Ensuite, le client s'authentifie auprès du serveur en utilisant généralement un couple identifiant/mot de passe. A la différence de la méthode EAP-TLS, cette méthode nécessite l'utilisation d'un seul certificat pour le serveur.
- EAP-TTLS : cette méthode se rapproche dans son fonctionnement de la méthode PEAP, a l'exception qu'elle nécessite la mise en place d'un serveur supplémentaire, le serveur TTLS. Celui-ci sera uniquement chargé de sécurisé les communications avec le client et servira d'intermédiaire entre ce dernier et le serveur d'authentification.

Le principe d'authentification du serveur RADIUS permet donc d'être réalisé selon différentes méthodes d'authentification. Dans le cas du système de vidéoprotection, ce sont les caméras IP qui devront s'authentifier auprès du serveur, il convient donc de savoir avec quel protocole ces équipements sont compatibles.

Les fiches techniques des modèles de caméra IP choisies pour la plateforme de test mentionnent une compatibilité avec le protocole EAP-TLS, ce sera donc ce protocole qui sera utilisé :

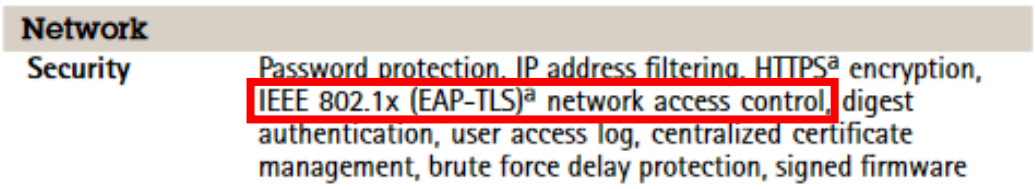

Figure 28 : Extrait de la fiche technique des caméras Axis précisant le type de protocole 802.1x pris en charge

3.3.2. Protocole EAP-TLS et Infrastructure de Gestion des Clés

La méthode d'authentification EAP-TLS repose donc sur le principe d'échange de certificats entre le supplicant et le serveur d'authentification pour que chacun puisse s'assurer de l'identité de l'autre.

La séquence des échanges et types de trames envoyées entre les différents équipements dans le cas de l'utilisation du protocole EAP-TLS est la suivante :

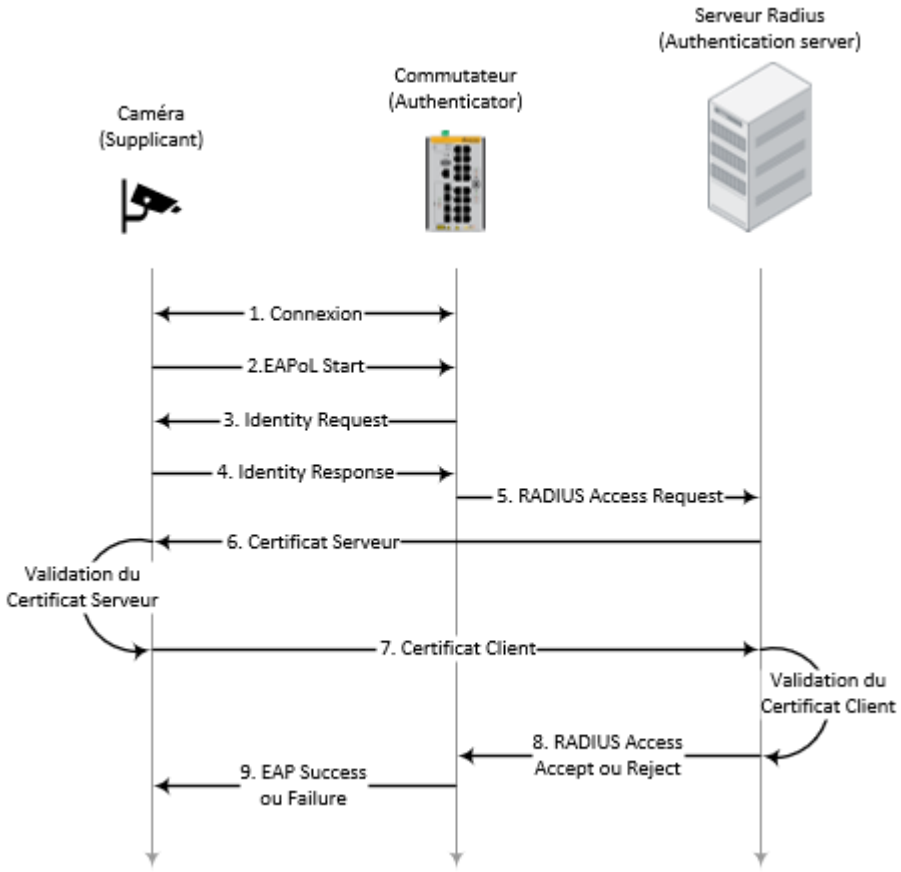

Figure 29 : Fonctionnement du mode EAP-TLS

Dans les étapes 1 et 2, la connexion entre le supplicant et le commutateur permet d'initialisé la session EAP.

S'ensuivent dans les étapes 3 et 4 la demande et le retour d'identité du supplicant qui retournera au commutateur le champ « User-Name » ainsi que le « Calling-Station-Id » correspondant à son adresse MAC.

Le commutateur peut alors envoyer au serveur d'authentification, lors de l'étape 5, une trame Access-Request avec les informations obtenues à l'étape 4.

Les étapes 6 et 7 consistent à l'échange et la validation des certificats entre le supplicant et le serveur, c'est ici que sont envoyées les trames Access-Challenge.

Enfin, lors des étapes 8 et 9, le serveur d'authentification accepte ou non la demande en retournant une trame Access-Accept ou Access-Reject au commutateur, qui passera alors son port en mode autorisé ou non autorisée en fonction de la réponse. Un retour d'information est également fait par le commutateur au supplicant via une trame EAP Success ou EAP Failure.

Pour permettre le fonctionnement du protocole RADIUS dans le mode EAP-TLS, il est donc nécessaire de mettre en place une Infrastructure de Gestion des Clé (IGC), organisation permettant la génération et le renouvellement des certificats qui seront installés dans le serveur RADIUS et les caméras IP [Bordères - 2006].
Le principe de fonctionnement de cette IGC est le suivant :

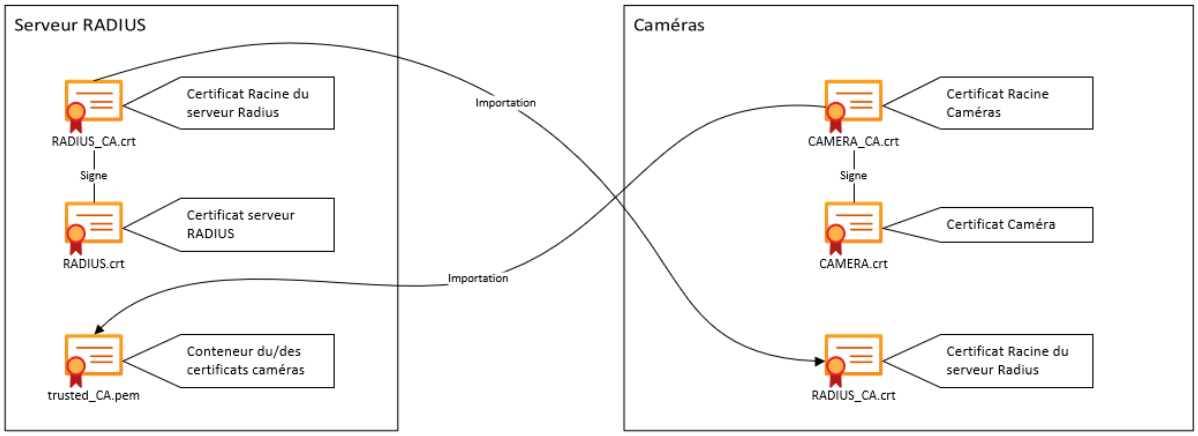

Figure 30 : Certificats nécessaires au fonctionnement du mode EAP-TLS

Deux certificats racine, également appelé Autorité de Certification (AC), sont créés, le premier pour le serveur RADIUS et le second pour les caméras. Ils serviront à signer respectivement le certificat du serveur RADIUS et les certificats des caméras.

Le certificat racine du serveur RADIUS est ensuite importé dans toutes les caméras comme certificat de confiance et le certificat racine des caméras est également importé comme certificat de confiance dans le serveur RADIUS. Chaque caméra est équipée d'un certificat qui lui est propre.

Lors des phases d'échanges illustrées dans la figure 29, à l'étape numéro 6, le certificat du serveur RADIUS est présenté à la caméra qui demande l'authentification sur le réseau. Cette dernière peut ainsi vérifier son authenticité grâce au certificat racine du serveur RADIUS qu'elle possède. Ensuite, à l'étape numéro 7, la caméra présente au serveur RADIUS son propre certificat, qui est alors authentifié par le serveur grâce au certificat racine des caméras qu'il possède. Cet échange est nommé dans la terminologie du protocole TLS le « handshake » [ANSSI - 2020b].

L'authentification est mutuelle, la caméra s'assurant dans un premier temps de l'identité du serveur RADIUS avant de lui délivrer son propre certificat, évitant ainsi une faille de sécurité au cas ou le serveur RADIUS aurait été remplacé par un serveur malveillant.

Selon les recommandations de L'ANSSI [ANSSI - 2020b], les certificats émis après le 1er mars 2018 doivent être générés pour une durée maximale de 825 jours. Ils doivent utiliser, toujours suivant les recommandations de l'ANSSI, des clés de chiffrement RSA de taille minimum de 2048 bits.

3.3.3. Mise en œuvre sur la plateforme de test

3.3.3.1. Création de l'IGC

Pour la création et la gestion de l'Infrastructure de Gestion des Clés, l'utilisation d'un logiciel graphique a été préférée à l'utilisation des lignes de commandes pour la génération des certificats.

En effet, cette gestion est souvent réalisée via l'utilisation du logiciel OpenSSL qui s'utilise en ligne de commande. Cette méthode n'est pas très intuitive et pourra être source d'erreur pour les personnes qui seront en charge d'assurer la maintenance du système en renouvelant les certificats.

Le choix a été fait d'utiliser XCA, logiciel libre et gratuit qui permet donc de créer une base de données de certificat en utilisant une interface graphique plus intuitive :

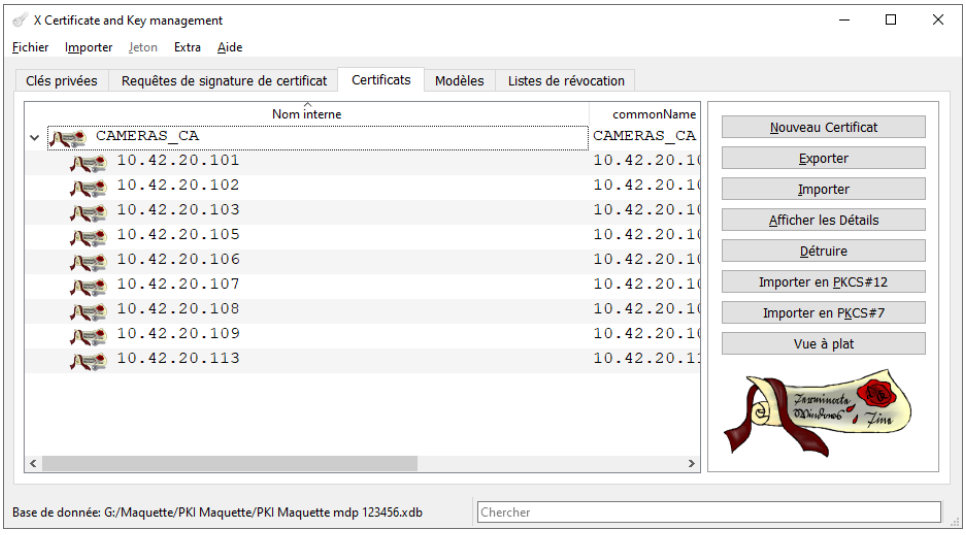

Figure 31 : Interface graphique du logiciel XCA

3.3.3.2. Installation et configuration du serveur RADIUS

L'installation du serveur RADIUS passe par l'installation du logiciel FreeRadius sur un serveur possédant le système d'exploitation Linux. Sur la plateforme de test, la distribution choisie est une version 20.04 LTS d'Ubuntu.

Le choix a été fait d'utiliser FreeRadius car c'est un logiciel gratuit et open source très répandu et qui est très bien documenté.

Pour installer le logiciel FreeRadius, il faut suivre les étapes suivantes [RADIUS - 2014] :

1) Taper la commande « `sudo apt-get update` » afin de mettre à jour les paquets d'installation
2) Taper la commande « `apt-get install freeradius` » afin de lancer l'installation de FreeRadius qui se fera ensuite de manière autonome

Il sera ensuite nécessaire de modifier plusieurs fichiers de configuration, qui se trouvent dans différents répertoire du dossier d'installation de FreeRadius, lui-même localisé sur le serveur dans « /etc/freeradius/3.0 » :

- client.conf : se fichier, se trouvant à la racine du répertoire d'installation, contiendra la liste des authentificateur autorisés à faire de requêtes d'accès au réseau auprès du serveur, en l'occurrence les commutateurs du réseau. Il faut renseigner dans ce fichier chaque commutateur en l'identifiant par son nom, son adresse IP ainsi qu'un mot de passe qui sera également saisi dans la configuration du commutateur :

```
client Switch_01 {
        ipaddr      = 10.42.30.12
        secret      = password
}
```

Figure 32 : Exemple d'entrée du fichier « client.conf » du serveur RADIUS

- eap : dans la configuration par défaut FreeRadius, le mode d'authentification est défini sur EAP-MD5. Il est nécessaire de changer cette configuration pour la remplacer par le mode EAP-TLS. Pour cela, il faut éditer le fichier « eap » se trouvant dans le répertoire « mods-available » du dossier d'installation de FreeRadius et modifier le champ « default_eap_type » pour lui affecter la valeur « tls »:

```
eap {
    #  Invoke the default supported EAP type when
    #  EAP-Identity response is received.
    #
    #  The incoming EAP messages DO NOT specify which EAP
    #  type they will be using, so it MUST be set here.
    #
    #  For now, only one default EAP type may be used at a time.
    #
    #  If the EAP-Type attribute is set by another module,
    #  then that EAP type takes precedence over the
    #  default type configured here.
    #
    default_eap_type = tls
```

Figure 33 : Modification du fichier « eap » du serveur RADIUS pour configuration du mode EAP-TLS

Il est également nécessaire, toujours dans le fichier « eap », d'indiquer le chemin d'accès et le nom des certificats utilisés par le serveur. Ces modification doivent être faite dans la section « tls-config tls-common » du fichier :

```
tls-config tls-common {
    private_key_password = whatever
    private_key_file = /etc/freeradius/3.0/certs/RADIUS.key

    #  If Private key & Certificate are located in
    #  the same file, then private_key_file &
    #  certificate_file must contain the same file
    #  name.
    #
    #  If ca_file (below) is not used, then the
    #  certificate_file below MUST include not
    #  only the server certificate, but ALSO all
    #  of the CA certificates used to sign the
    #  server certificate.
    certificate_file = /etc/freeradius/3.0/certs/RADIUS.crt

    #  Trusted Root CA list
    #
    #  ALL of the CA's in this list will be trusted
    #  to issue client certificates for authentication.
    #
    #  In general, you should use self-signed
    #  certificates for 802.1x (EAP) authentication.
    #  In that case, this CA file should contain
    #  *one* CA certificate.
    #
    ca_file = /etc/freeradius/3.0/certs/CAMERA_CA.pem
```

Figure 34 : Modification du fichier « eap » du serveur RADIUS pour localisation des certificats

Le champ « private_key_file » doit spécifier le chemin d'accès au fichier contenant la clé privée du certificat du serveur et le champ « private_key_password » le mot de passe d'encryptage de cette clé. Le champ « certificate_file » doit quant à lui indiquer le chemin d'accès au certificat du serveur.

Enfin, il faut préciser dans le champ « ca_file » le chemin d'accès au certificat racine des caméras.

3.3.3.3. Configuration des commutateurs et du routeur firewall

Le serveur RADIUS sera intégré à l'infrastructure du système dans la partie serveur, il fera donc parti du VLAN n°20 :

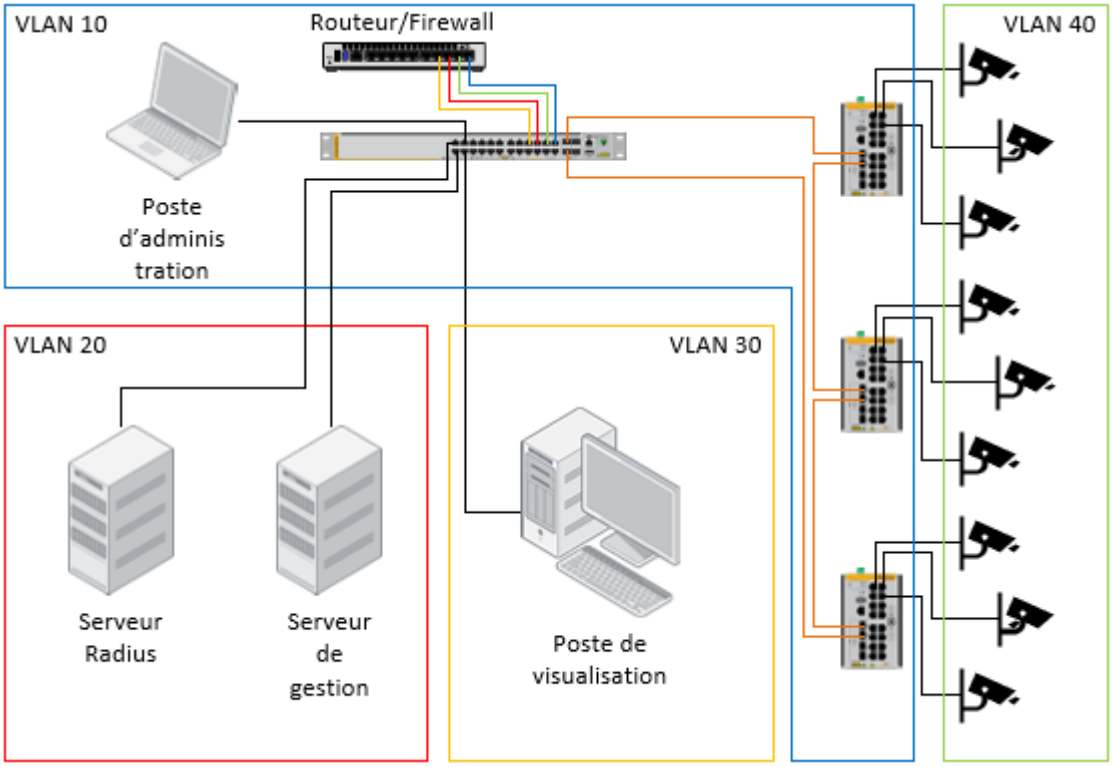

Figure 35 : Intégration du serveur RADIUS au réseau

Pour réaliser la configuration du protocole RADIUS dans les commutateurs, il sera nécessaire de suivre les étapes suivantes [Allied - 2021b] :

1) Se connecter à l'interface d'administration du commutateur.
2) Taper la commande « `enable` » afin d'activer la console.

3) Taper la commande « `configure terminal` » pour entrer en mode configuration.

Ces trois premières commandes sont à exécuter à chaque connexion au commutateur pour entrer en mode configuration.

4) Taper la commande « `radius-server host x.x.x.x key password` » pour ajouter le serveur RADIUS au commutateur, en remplaçant x.x.x.x par l'adresse IP du serveur RADIUS et password par le mot de passe renseigné pour ce même commutateur dans le fichier « client.conf » du serveur RADIUS.
5) Taper la commande « `aaa authentication dot1x default group radius` » pour indiquer au commutateur d'utiliser le serveur RADIUS ajouté précédemment afin qu'il puisse lui envoyer les demandes d'authentification.

Ensuite, pour chaque port sur lequel sera raccordé un équipement qui nécessitera une authentification, il faudra exécuter les commandes suivantes :

1) Taper la commande « `interface port1.0.xx` » en remplaçant xx par le numéro du port à configurer
2) Taper la commande « `dot1x port-control auto` »

Concernant la configuration du routeur firewall, les flux réseaux nécessaires ont été ajoutés dans la matrice des flux du tableau XXVII page 63. Il faudra alors ajouter le serveur RADIUS dans la section Addresses, les ports dans la section Services et enfin créer les règles de routage dans la section IPv4 Policy.

3.3.3.4. Configuration des caméras IP

La configuration des caméras IP se réalise directement depuis l'interface de gestion web de ces dernières. Dans l'onglet « Système » puis « Sécurité », il faudra réaliser les étapes suivantes :

1) Importer le certificat racine du serveur RADIUS généré précédemment
2) Importer le certificat propre à la caméra
3) Indiqué le nom de la caméra qui sera envoyé au serveur RADIUS dans le champs « Identité EAP »
4) Activer l'utilisation du protocole RADIUS en cochant la case « Utiliser IEEE 802.1x »

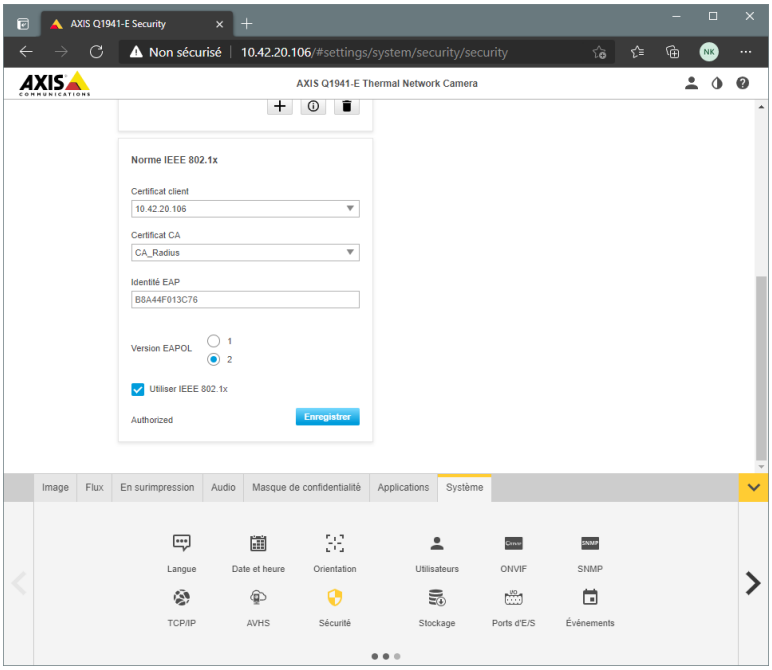

Figure 36 : Page web de configuration des fonctionnalités 802.1x des caméras IP

3.3.3.5. Test de fonctionnement

La vérification du fonctionnement de l'authentification RADIUS peut se faire directement depuis la console du logiciel FreeRadius lancée en mode « debug ». Pour lancer le service FreeRadius dans ce mode, il faut exécuter la commande « sudo freeradius -x -XX » dans le terminal du serveur. Le journal des événements s'affiche et il est alors possible de suivre les échanges entre les commutateurs et le serveur RADIUS.

Lors de la connexion d'une caméra sur un des ports configuré du commutateur, les messages suivants s'affichent :

1) Demande d'authentification de la caméra :

```
Fri Apr 30 08:21:15 2021 : Debug: (0) Received Access-Request Id 42 from 10.42.30.12:55365 to 10.42.30.150:1812 length 133
Fri Apr 30 08:21:15 2021 : Debug: (0)   User-Name = "B8A44F013B6F"
Fri Apr 30 08:21:15 2021 : Debug: (0)   Framed-MTU = 1500
Fri Apr 30 08:21:15 2021 : Debug: (0)   NAS-IP-Address = 10.42.30.12
Fri Apr 30 08:21:15 2021 : Debug: (0)   NAS-Port = 5012
Fri Apr 30 08:21:15 2021 : Debug: (0)   NAS-Port-Type = Ethernet
Fri Apr 30 08:21:15 2021 : Debug: (0)   Called-Station-Id = "00-0c-25-2b-07-4f"
Fri Apr 30 08:21:15 2021 : Debug: (0)   Calling-Station-Id = "b8-a4-4f-01-3b-6f"
```

Figure 37 : Extrait du journal du serveur RADIUS "Access-Request"

Dans cette partie du journal on retrouve la demande d'authentification de la caméra « Access-Request » avec les champs :

- User-Name : correspond au nom d'utilisateur configuré dans l'interface web de la caméra
- NAS-IP-Address : il s'agit du commutateur à l'origine de la requête
- Called-Station-Id : correspond à l'adresse MAC du commutateur à l'origine de la requête
- Calling-Station-Id : correspond à l'adresse MAC de la caméra à l'origine de la requête

2) Réponse du serveur RADIUS à la demande d'authentification :

```
Fri Apr 30 08:21:15 2021 : Debug: (0) Sent Access-Challenge Id 42 from 10.42.30.150:1812 to 10.42.30.12:55365 length 0
Fri Apr 30 08:21:15 2021 : Debug: (0)   EAP-Message = 0x010200060d20
Fri Apr 30 08:21:15 2021 : Debug: (0)   Message-Authenticator = 0x00000000000000000000000000000000
Fri Apr 30 08:21:15 2021 : Debug: (0)   State = 0x88c1c39e88c3ce4f581e3c112c245f6f
Fri Apr 30 08:21:15 2021 : Debug: (0) Finished request
```

Figure 38 : Extrait du journal du serveur RADIUS "Access-Challenge"

Le serveur RADIUS retourne alors un message « Access-Challenge » qui va initier l'échange des certificats entre le serveur et la caméra.

3) Echange des certificats :

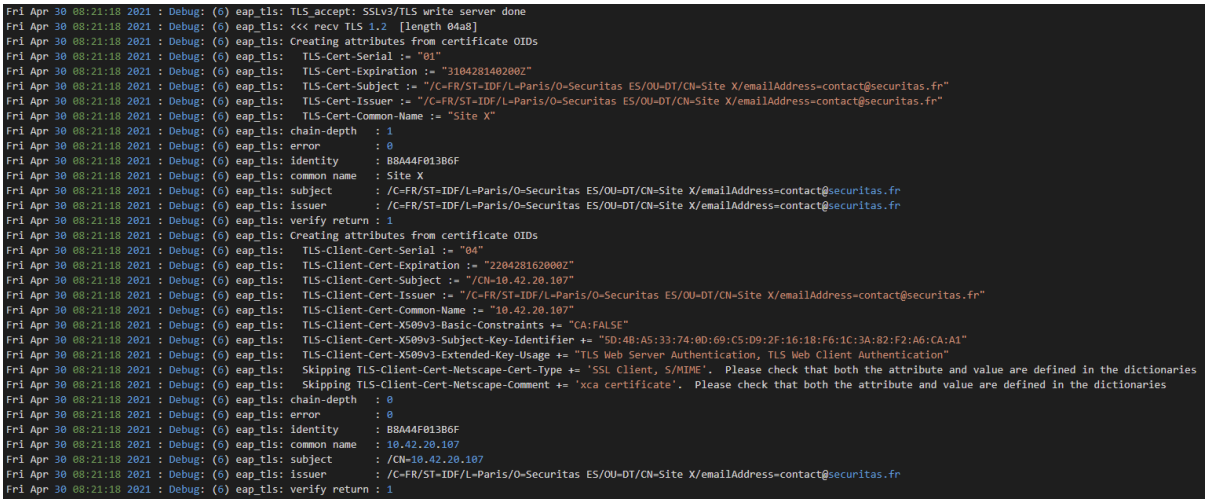

Figure 39 : Extrait du journal du serveur RADIUS - échange des certificats

Dans cette partie du journal on retrouve l'échange des certificats entre le serveur RADIUS et la caméra.

4) Acceptation ou refus de la requête par le serveur RADIUS :

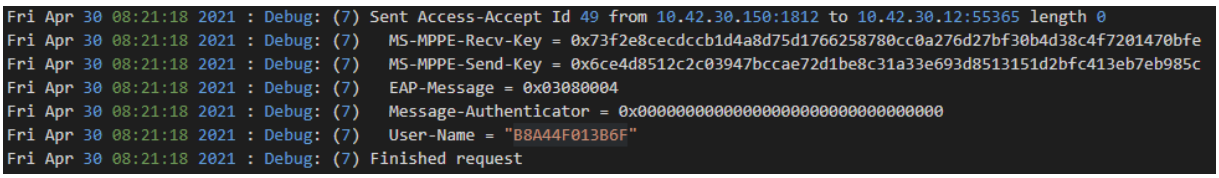

Figure 40 : Extrait du journal du serveur RADIUS "Access-Accept"

Dans le cas où les certificats échangés ont pu être authentifiés avec succès, le message « Access-Accept » est envoyé par le serveur RADIUS au commutateur.

La requête est alors acceptée, la caméra se retrouve connectée au réseau et les échanges entre le serveur RADIUS et le commutateur s'arrêtent.

Dans le cas où les certificats ne sont pas valides, le serveur l'indique par le message d'erreur « sslv3 alert bad certificate » :

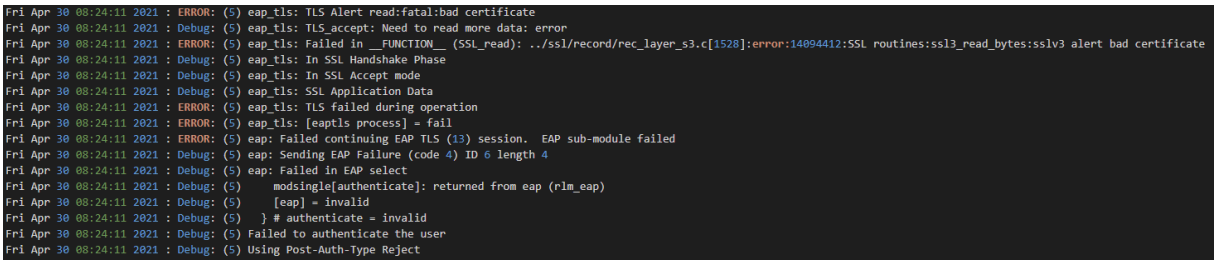

Figure 41 : Extrait du journal du serveur RADIUS "sslv3 alert bad certificate"

Le message « Access-Reject » est alors retourné par le serveur RADIUS au commutateur. La requête est refusée, la caméra ne peut pas accéder au réseau et les échanges entre le serveur RADIUS et le commutateur s'arrêtent :

```
Fri Apr 30 08:24:12 2021 : Debug: (5) Sent Access-Reject Id 55 from 10.42.30.150:1812 to 10.42.30.12:55365 length 44
Fri Apr 30 08:24:12 2021 : Debug: (5)   EAP-Message = 0x04060004
Fri Apr 30 08:24:12 2021 : Debug: (5)   Message-Authenticator = 0x00000000000000000000000000000000
```

Figure 42 : Extrait du journal du serveur RADIUS "Access-Reject"

4. Intégration dans les projets

L'intégration de ces mesures de sécurité dans les projets de vidéoprotection réalisés par Securitas Sécurité Electronique va représenter un coût et nécessitera des prérequis technique des équipements et une méthode spécifique.

4.1. Coût d'intégration

L'essentiel des coûts induits par l'application des mesures de sécurité se portera sur les équipements additionnels nécessaires ainsi que sur la main d'œuvre supplémentaire utile à la configuration du système.

Ces coûts sont estimés dans le tableau ci-dessous, ils serviront au service commerciale afin d'établir les devis pour les clients nécessitant ces mesures de sécurité sur leur réseau dédié au système de vidéoprotection. Les temps de main d'œuvre estimés dans ce tableau viendront s'ajouter à ceux habituellement nécessaires à l'installation et la configuration des équipements. Ils sont estimés grâce au retour d'expérience de la mise en œuvre des configurations sur la plateforme de test.

Tableau XXVIII: Estimation des coûts induits par la mise en œuvre des mesures de sécurité

Equipement ou prestation	Prix d'achat ou durée en heure
Routeur firewall (estimation basée sur le prix d'un routeur firewall Fortinet Fortigate 60E + kit d'installation en baie)	Environ 900€ HT
Configuration de base du routeur firewall (y compris recherches nécessaire à l'élaboration de la matrice des flux)	8 heures
Serveur RADIUS (estimation basée sur le prix d'un serveur DELL Poweredge R340)	Environ 2500€ HT
Installation et configuration du serveur RADIUS (y compris génération des certificats racines)	16 heures
Configuration de base des commutateurs réseau (y compris ajout à la liste des commutateurs autorisés du serveur RADIUS)	1 heure par commutateur
Configuration supplémentaire par caméras (comprend la configuration du port associé du commutateur, la configuration du routage des flux dans le routeur firewall ainsi que la génération et la mise en place du certificat)	½ heure par caméra

Dans le cadres des contrats de maintenance passés avec les clients pour l'entretient de leur système de vidéoprotection, il faudra également ajouter un quart d'heure par caméra pour le renouvellement des certificats au temps de main d'œuvre généralement nécessaire à l'entretient de ces dernières.

4.2. Prérequis et méthode

Pour les prérequis techniques des équipements, il faudra respecter les besoins suivants :

- Les caméras IP devront être compatible avec la norme IEEE 802.1x, plus particulièrement compatibles avec le protocole EAP-TLS, pour l'intégration du protocole RADIUS.
- Les commutateurs réseaux devront également être compatible avec la norme IEEE 802.1x et le protocole EAP-TLS, mais également avec la norme IEEE 802.1Q pour l'intégration des VLAN.
- Le routeur firewall devra être adapté au nombre de caméras IP présentes dans l'installation, en effet la bande passante des caméras IP n'est pas négligeable, et les capacités techniques d'un routeur firewall impose une limite à la bande passante totale transitant par le firewall.

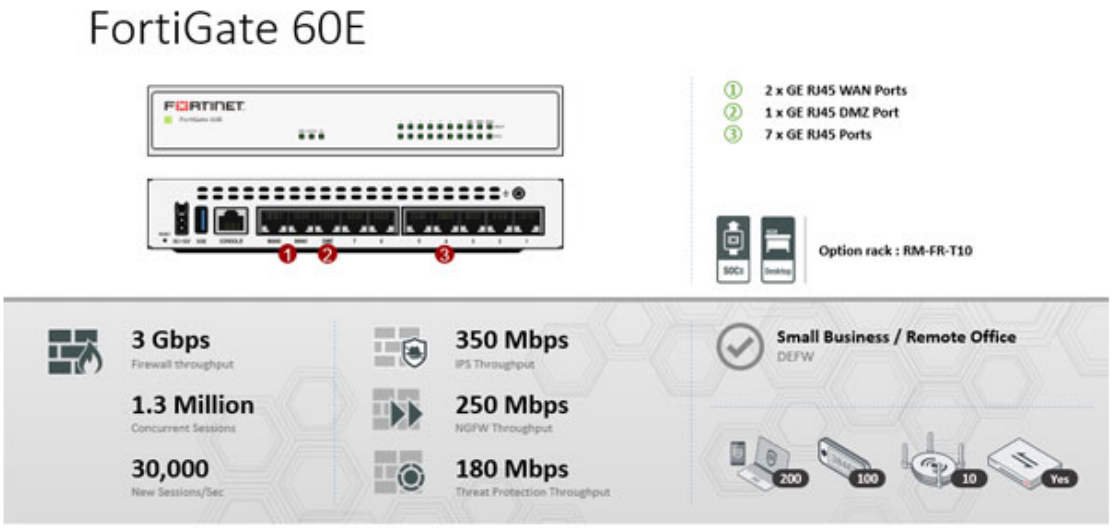

Figure 43: Extrait des caractéristiques techniques du routeur firewall Fortinet Fortigate 60E

La figure 25, extraite des caractéristiques techniques d'un routeur firewall Fortinet Fortigate 60E, indique une limite à 3 Gbps de la bande passante maximale admissible par le firewall. Le volume de la bande passante des équipements du système ne devra pas dépasser cette limite.

Concernant l'intégration des mesures de sécurité dans les systèmes de vidéoprotection déployés, les procédures suivantes ont été rédigées :

- Installation et configuration du serveur RADIUS : cette procédure contient l'intégralité des étapes nécessaires à l'installation du serveur RADIUS, en partant de l'installation de la distribution Ubuntu de Linux jusqu'à l'installation et la configuration du logiciel FreeRadius
- Création et gestion de l'Infrastructure de Gestion des Clés : cette procédure détaille les étapes nécessaires à la génération des certificats, grâce au logiciel XCA, dans le cadre de l'utilisation du logiciel FreeRadius, mais également la révocation de ces derniers en cas de remplacement d'une caméra IP et leurs renouvellement dans le cadre de la maintenance du système
- Configuration des switch Allied Telesis (VLAN et mesures de sécurité) : cette procédure explique les étapes nécessaire à la mise en service des commutateurs de la marque Allied Telesis, plus particulièrement la création des VLAN et l'activation des mesures de sécurité de base, mais également la configuration du commutateurs et des ports nécessaires à l'utilisation du protocole RADIUS
- Configuration du routeur firewall Fortinet Fortigate 60 E : cette procédure détaille la mise en service et la configuration étape par étape du routeur firewall, notamment la création des interfaces et des règles de routage

Ces procédures, notamment celles concernant les commutateurs et le routeur firewall, sont spécifiques aux équipements utilisés dans la plateforme de test mise en œuvre dans le cadre de ce mémoire. Elles devront être adaptés en fonction des fabricants et des modèles d'équipements utilisés dans les autres projets d'installation de systèmes de vidéoprotection.

Conclusion

La réalisation de ce projet a permis de mettre en évidence les besoins de sécurité des systèmes d'informations dédié à la vidéoprotection et a permis de faire évoluer la maturité de l'entreprise en terme de cybersécurité.

L'analyse de risque informatique, conduite via l'utilisation de la méthode EBIOS RM, a permis d'identifier le socle de sécurité à mettre en œuvre sur ces systèmes en étudiant les différents référentiels et guides de recommandations applicables. Cette partie du projet à également permis d'acquérir la méthode de conduite de telles analyses de risque, qui pourra être reproduite sur d'autres systèmes internes ou externes à l'entreprise.

L'étude des mesures de sécurité propres au réseau du système, ainsi que leurs applications sur une plateforme de test composée des équipements généralement utilisés dans les systèmes de sécurité déployés par Securitas Sécurité Electronique, ont permis de confirmer d'une part leurs faisabilité technique et d'autre part de créer des procédures d'installation et de configuration. Ces procédures permettrons aux équipes techniques de l'entreprise de reproduire ces configurations lors de la réalisation des projets chez nos clients.

Enfin, l'estimation des coûts d'intégration et des prérequis techniques nécessaires à l'application de ces mesures de sécurité dans les projets permettra à l'équipe commerciale de l'entreprise de construire les devis pour nos clients en sélectionnant les bons matériels et logiciels et en appliquant les bons temps de main d'œuvre requis pour leurs installations et configurations.

L'étude s'est toutefois portée dans sa partie technique uniquement sur le réseau du système. Dans la continuité de ce projet, il sera intéressant d'étudier à l'avenir les mesures de sécurité qui ont été identifiés et qui portent sur la sécurisation des autres composant du système, tels que les serveurs de gestion ou les postes de visualisation.

De plus, dans une démarche d'amélioration continue, il conviendra de suivre l'évolution des référentiels et des guides de recommandations pour continuer de perfectionner la sécurité des systèmes d'information mis en œuvre par l'entreprise.

Bibliographie

[Bordères - 2006] : BORDERES S, 2006. Authentification réseau avec Radius. Eyrolles, 210p.

[CNPP - 2017] : CNPP, 2017. Référentiel APSAD D32. Cybersécurité. Document technique pour l'installation de systèmes de sécurité ou de sûreté sur un réseau informatique. Edition de juin 2017. CNPP, 40p.

[Ghernaouti - 2019] : GHERNAOUTI S, 2019. Cybersécurité. Analyser les risques. Mettre en œuvre les solutions. 6e édition. Dunod, 391 p.

[Llorens et al. - 2010] : LLORENS C, LEVIER L, VALOIS D, MORIN B, 2010. Tableau de bord de la sécurité réseau. 3e édition. Eyrolles, 561 p.

[Lohier et Présent - 2020] : LOHIER S, PRESENT D, 2020. Réseaux et transmissions. Protocoles, infrastructures et services. 7e édition. Dunod, 326p.

Webographie

[Allied - 2021a] : Allied Telesis, 2021. Virtual LANs. Feature Overview and Configuration Guide. Révision M, 2021. Disponible sur https://www.alliedtelesis.com/fr/documents/vlans-feature-overview-and-configuration-guide

[Allied - 2021b] : Allied Telesis, 2021. AAA and Port Authentication. Feature Overview and Configuration Guide. Révision J, 2021. Disponible sur https://www.alliedtelesis.com/fr/documents/aaa-and-port-authentication-feature-overview-and-configuration-guide

[ANSSI - 2016] : ANSSI, 2016. Recommandations pour la sécurisation d'un commutateur de desserte. Version 1.0 de juin 2016. Disponible sur https://www.ssi.gouv.fr/

[ANSSI - 2017] : ANSSI, 2017. Guide d'hygiène informatique. Version 2.0 de septembre 2017. Disponible sur https://www.ssi.gouv.fr/

[ANSSI - 2018a] : ANSSI, 2018. Guide méthode EBIOS Risk Manager. Version 1.1 de décembre 2018. Disponible sur https://www.ssi.gouv.fr/

[ANSSI - 2018b] : ANSSI, 2018. Fiches méthode EBIOS Risk Manager. Version 1.1 de janvier 2019. Disponible sur https://www.ssi.gouv.fr/

[ANSSI - 2018c] : ANSSI, 2018. Recommandations de déploiement du protocole 802.1x pour le contrôle d'accès à des réseaux locaux. Version 1.0 d'août 2018. Disponible sur https://www.ssi.gouv.fr/

[ANSSI - 2020a] : ANSSI, 2020. Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection. Version 2.0 de mars 2020. Disponible sur https://www.ssi.gouv.fr/

[ANSSI - 2020b] : ANSSI, 2020. Recommandations de sécurité relatives à TLS. Version 1.2 de mars 2020. Disponible sur https://www.ssi.gouv.fr/

[CLUB EBIOS - 2021] : Club EBIOS, 2021. Filtrage du référentiel ATT&CK pour outiller la construction de scénarios opérationnels. Version 1.01 de janvier 2021. Disponible sur https://club-ebios.org/site/selecteur-de-techniques-dattaque-outillage-pour-latelier-4/

[FORTINET - 2021] : Fortinet, 2021. Fortigate FortiOS 7.0.0 Administration Guide. Disponible sur https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/954635/getting-started

[MILESTONE - 2021] : Milestone, 2021. XProtect VMS Administrator Manual. Version 2020. Disponible sur https://doc.milestonesys.com/2020r3/en-US/portal/htm/chapter-page-mc-administrator-manual.htm?tocpath=XProtect%20VMS%20products%7CXProtect%20VMS%20Administrator%20manual%7C_____0

[RADIUS - 2014] : RADIUS SARL, 2014. The FreeRADIUS Technical Guide. Version de 2014. Disponible sur https://freeradius.org/documentation/

Mémoire présenté en vue d'obtenir le diplôme d'Ingénieur CNAM

Spécialité : INFORMATIQUE parcours Systèmes d'Information

Lyon, 2021

Résumé

La sécurité des systèmes d'information est au cœur de toutes les préoccupations de nos jours. Les systèmes de sécurité de type vidéoprotection, systèmes d'information à part entière, n'échappent pas aux besoins de sécurité informatique.
Une analyse de risque, réalisée via la méthode EBIOS Risk Manager permet d'identifier les risques qui pèsent sur ces systèmes ainsi que les mesures de sécurité à appliquer.
La mise en œuvre de ces mesures de sécurité est ensuite étudiée, plus précisément celles concernant le réseau support du système. Sont ainsi analysés le cloisonnement du réseau via la mise en place de VLAN et le contrôle d'accès par l'utilisation du protocole RADIUS.

Mots clé : Cybersécurité – Vidéoprotection – Analyse de risque – EBIOS RM – Cloisonnement – VLAN – Contrôle d'accès – RADIUS

Abstract

The security of information systems is at the heart of all concerns these days. Security systems of the video protection type, information systems in their own right, are no exception to IT security needs.
A risk analysis, carried out using the EBIOS Risk Manager method, identifies the risks weighing on these systems as well as the security measures to be applied.
The implementation of these security measures is then studied, more precisely those concerning the system network. The partitioning of the network through the implementation of VLANs and access control through the use of the RADIUS protocol are thus analyzed.

Keywords: Cybersecurity – Video protection – Risk analysis – EBIOS RM – Partitioning – VLAN – Access control - RADIUS