



**SECURE-IP**

# BTS SIO Option SLAM 2022-2023

SECURE-IP

EYMARD IOV

## Table des matières

<b>INTRODUCTION .....</b>	<b>1</b>
<b>1)PRESENTATION DE L'ENTREPRISE .....</b>	<b>2</b>
1.1) POINTS CLES DE L'ENTREPRISE .....	2
1.2) PRESENTATION DE L'ACTIVITE DE L'ENTREPRISE .....	3
1.3) ORGANIGRAMME FONCTIONNEL DE L'ENTREPRISE .....	4
1.4) PRESENTATION DE L'ORGANISATION INTERNE ET EXTERNE.....	5
<b>2) MA CONTRIBUTION DANS L'ENTREPRISE .....</b>	<b>6</b>
2.1) MON INTEGRATION DANS L'ENTREPRISE .....	6
2.2) MES MISSIONS ET OBJECTIF .....	7
<b>3) DEROULEMENT DE L'APPRENTISSAGE .....</b>	<b>8</b>
3.1) COMPRENDRE VXCORE .....	9
3.2) COMPRENDRE COMMENT FONCTIONNE LES EQUIPEMENTS DU CONTROLE D'ACCES .....	10
3.3) COMPRENDRE LA CENTRALE D'ALARME .....	11
3.4) LA SYNERGIE ENTRE TOUS CES EQUIPEMENTS .....	13
3.5) PREPARATIONS DE TOUS SES EQUIPEMENTS .....	14
3.6) MAINTENANCE DE SES EQUIPEMENT ET AMELIORATIONS.....	15
<b>4) COLLABORATION ET COMMUNICATION DURANT L'APPRENTISSAGE.....</b>	<b>19</b>
4.1) REPORTING .....	19
4.2) COMMUNICATION AVEC LE MAITRE DE STAGE .....	19
4.3) COMMUNICATION AVEC D'AUTRES COLLABORATEUR .....	20
<b>5) COMPETENCES ACQUISES CORRESPONDANT A L'EPREUVE E4 DU BTS .....</b>	<b>21</b>
5.1) GERER LE PATRIMOINE INFORMATIQUE .....	21
5.2) REPONDRE AUX INCIDENTS ET AUX DEMANDES D'ASSISTANCES ET D'EVOLUTIONS .....	22
5.3) METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE .....	24
<b>CONCLUSION .....</b>	<b>25</b>
<b>GLOSSAIRE TECHNIQUE .....</b>	<b>26</b>

## Introduction

Ce document constitue le rapport d'apprentissage relatif à ma première et deuxième année d'alternance au sein de Secure-IP, effectuée du 03 novembre 2022 au 20 Août 2024, dans le cadre de ma formation en BTS Services Informatiques aux Organisations (option solutions logicielles et applications métiers). Au cours de cette période de professionnalisation, j'ai occupé le poste d'alternant en support et réseau.

## 1)Présentation de l'entreprise

L'analyse de l'entreprise est une étape cruciale pour comprendre son environnement, ses activités et son fonctionnement interne et externe. Dans cette section nous allons explorer en détail Secure-IP, en examinant son secteur d'activité, ses produits, ses services, ses principaux concurrents, ainsi que son organisation interne et externe.

### 1.1) Points clés de l'entreprise

- Secure-IP est une PME proposant des solutions de vidéo protection et de contrôle d'accès
- Basée à Massy-Palaiseau (91300)
- 15 employées
- 3,2 millions d'euro de chiffre d'affaires en 2023
- Site web: <https://www.secure-ip.fr/>

## 1.2) Présentation de l'activité de l'entreprise

Secure-IP c'est propose ces différents services :

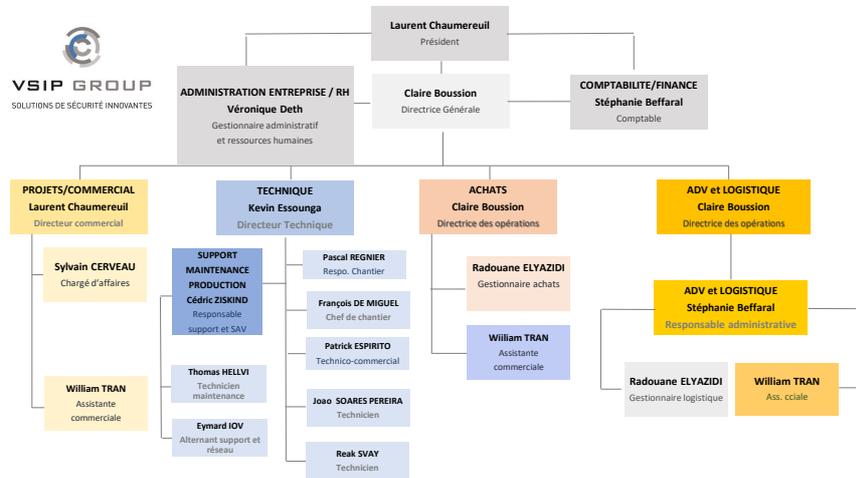
- Alarme anti-intrusion
- Vidéo protection
- Contrôle d'accès
- Maintenance de ces services

Client de différents secteurs :

Espaces de travail  
Site de production  
Associations

Les concurrents de Secure-IP incluent ses propres fournisseurs qui disposent d'un département d'installation : Salto, Simon Voss.

### 1.3) Organigramme fonctionnel de l'entreprise



#### 1.4) Présentation de l'organisation interne et externe

Le processus de décision chez Secure-IP est généralement effectué par le président et/ou la directrice générale. Les décisions stratégiques sont prises par les mêmes personnes, tandis que les décisions opérationnelles sont prises par les responsables de chaque département. En termes de pratiques managériales, Secure-IP a une culture d'entreprise axée sur l'innovation, la collaboration et l'excellence opérationnelle. L'entreprise encourage la formation et le développement professionnel de ses employés. L'entreprise façonne une culture fondée sur l'innovation et la collaboration.

Durant mon apprentissage, j'ai été affecté au support et à la production des solutions proposées.

## 2) Ma contribution dans l'entreprise

### 2.1) Mon intégration dans l'entreprise

Mon intégration au sein de Secure-IP a été facilitée par un environnement accueillant et une équipe de professionnels dévoués. Sous la tutelle de mon directeur technique, j'ai été chaleureusement accueilli et présenté à des collègues clés, ce qui m'a permis de m'adapter rapidement aux procédures et méthodes de travail propres à l'entreprise. Cependant, j'ai été confronté à des défis lors de ma collaboration avec les techniciens, principalement en raison de la rareté des interactions directes, limitant ainsi les retours et les opportunités d'amélioration.

Malgré ces obstacles, ma détermination et mon autonomie m'ont permis de surmonter ces difficultés et de m'intégrer avec succès dans l'équipe.

## 2.2) Mes missions et objectif

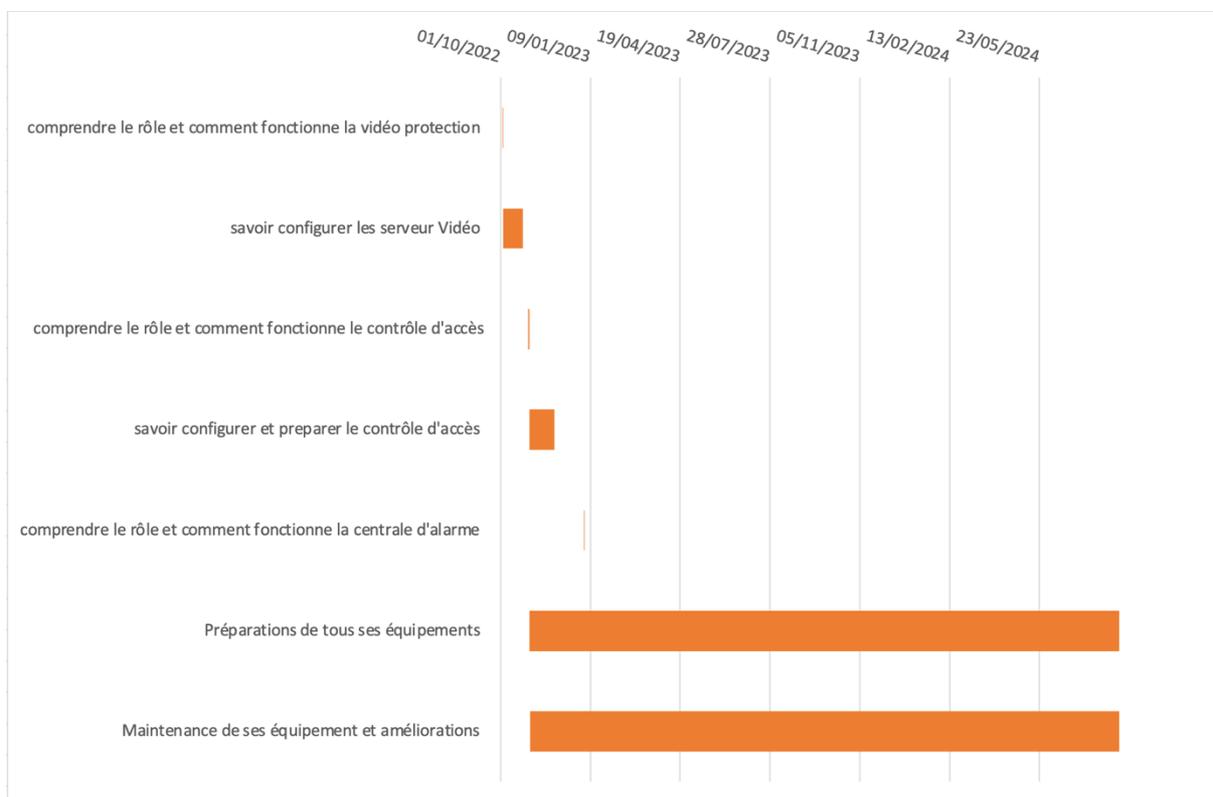
En tant qu'apprenti opérateur informatique chez Secure-IP, mes missions principales étaient :

- Préparations des équipements de vidéosurveillance
- Préparations du matériel lié au contrôle d'accès
- Aide à la maintenance des équipements sur site ou à distance
- Création ou améliorations de tâches automatisées

### 3) Déroulement de l'apprentissage

Mon apprentissage s'est déroulé en plusieurs étapes :

- 1 Premièrement de comprendre le rôle et comment fonctionne la vidéo protection
- 2 Ensuite de même pour le contrôle d'accès
- 3 Pareil pour les centrales d'alarmes
- 4 appréhender la complaisions de ces équipements
- 5 Préparations de tous ses équipements
- 6 Maintenance de ses équipement et améliorations



### 3.1) Comprendre Vxcore

VxCore d'Arcane représente un ensemble de software et OS spécialisé dans la surveillance vidéo, offrant une panoplie de fonctionnalités dédiées à la sécurité. Ce système comprend une interface utilisateur soigneusement conçue pour permettre aux opérateurs de surveiller efficacement les flux vidéo en temps réel et d'accéder facilement aux enregistrements antérieurs. La gestion des ressources matérielles telles que les caméras de sécurité, les disques de stockage et les réseaux est optimisée pour assurer un fonctionnement fluide et fiable du système de surveillance. Des mesures de sécurité robustes sont intégrées pour protéger les flux vidéo, les enregistrements et les données des utilisateurs contre les accès non autorisés et les violations de la confidentialité. De plus, VxCore offre des options de personnalisation pour répondre aux besoins spécifiques des utilisateurs finaux. Arcane assure également un support technique complet et des politiques de maintenance régulières pour garantir le bon fonctionnement et la sécurité à long terme du système VxCore. En somme, comprendre VxCore d'Arcane nécessite une exploration approfondie de ses fonctionnalités de surveillance vidéo, de son interface utilisateur, de sa gestion des ressources, de ses mesures de sécurité, de ses options d'intégration et de personnalisation, ainsi que de son support et de sa maintenance.

### 3.2) Comprendre comment fonctionne les équipements du contrôle d'accès

Comprendre le fonctionnement des équipements de contrôle d'accès tels que ceux de Salto ou Simon Voss implique d'explorer les mécanismes sophistiqués déployés pour sécuriser les entrées physiques des bâtiments. Ces équipements reposent sur une combinaison de technologies matérielles et logicielles pour réguler les accès de manière efficace et sécurisée. Tout d'abord, le système identifie les utilisateurs autorisés à l'aide de diverses méthodes telles que les cartes RFID ou, les badges, mais aussi si l'équipement le permet, les smartphones équipés de la technologie NFC. Une fois l'utilisateur identifié, le système communique avec un contrôleur central, souvent via des connexions câblées, mais possible aussi sans fil, pour vérifier les autorisations d'accès. Ces autorisations sont gérées via un logiciel centralisé qui permet aux administrateurs de définir et de modifier les droits d'accès en fonction des rôles et des niveaux d'autorisation de chaque utilisateur. Parallèlement, le système enregistre toutes les tentatives d'accès, réussies ou non, permettant une surveillance continue et une analyse ultérieure des activités à des fins de sécurité et de gestion. Les composants matériels du système, tels que les serrures électroniques et les lecteurs de cartes, sont conçus pour résister aux tentatives de contournement ou de manipulation non autorisées. Enfin, ils peuvent être intégrés à d'autres systèmes de sécurité ou de gestion des bâtiments. En synthèse, la compréhension de cet équipement implique d'explorer les méthodes d'identification, les protocoles de communication, la gestion des autorisations, la sécurité physique et les intégrations avec d'autres systèmes pour garantir un contrôle d'accès efficace et sécurisé des bâtiments.

### 3.3) Comprendre la centrale d'alarme

Comprendre le fonctionnement des centrales d'alarme, telles que celles de Vanderbilt, est essentiel pour assurer la sécurité des bâtiments. Ces centrales jouent un rôle central dans la surveillance et la gestion des incidents liés à la sécurité.

Les centrales d'alarme surveillent en permanence les capteurs installés dans le bâtiment, tels que les détecteurs d'ouverture de porte. En cas de détection d'un événement indésirable, comme une intrusion ou un incendie, la centrale d'alarme déclenche des actions appropriées pour répondre à la situation. Ces actions peuvent conduire à l'activation de protocoles préétablis pour assurer la sécurité des personnes et des biens. Les centrales d'alarme offrent également des fonctionnalités avancées telles que la surveillance à distance et la gestion centralisée des systèmes de sécurité sur SPC Connect Pro. Les responsables de sécurité peuvent surveiller l'état des systèmes en temps réel, recevoir des alertes en cas d'incident sur MyHorus et effectuer des actions de maintenance à distance, telles que la mise à jour du firmware des équipements.

En résumé, les centrales d'alarme sont un élément essentiel des systèmes de sécurité des bâtiments. Elles surveillent en permanence les capteurs et déclenchent des actions appropriées en cas d'incident pour assurer la sécurité des occupants et des biens. Avec des fonctionnalités avancées telles que la surveillance à distance et la gestion centralisée, les centrales d'alarme permettent une gestion efficace des systèmes de sécurité dans les environnements résidentiels, commerciaux et industriels.

## SPC Connect Pro :

The screenshot shows the SPC Connect Pro interface. The main content area displays a table of central units (Centrales) with the following columns: Nom de la centrale, Nom du site, Version du firmware, Connectée, Modifier la centrale, Tester Connexion, Se connecter, Licences de centrales, Opérations, and Supprimer la centrale. The table lists 12 units, each with its specific ID, site name, address, and connection status (e.g., OK 16:43:08).

## MyHorus :

The screenshot shows the MyHorus interface. The main content area displays a table of sites (Sites) with the following columns: Références, Prom, Nom, Code Postal, Ville, Id client, Contact, Adresse 1, Adresse 2, Complément d'adresse, and Pr. The table lists 18 sites, each with its specific reference, promotion, name, postal code, city, client ID, contact, address, and completion status (e.g., EN ATTENTE).

### 3.4) La synergie entre tous ces équipements

Les équipements de contrôle d'accès, de vidéo surveillance et la centrale d'alarme se complètent parfaitement pour offrir une protection globale et réactive des sites en fonction des besoins et des horaires d'activité des clients, sous certaines conditions.

Premièrement, le contrôle d'accès permet de réguler l'accès physique aux bâtiments en identifiant les utilisateurs autorisés et en restreignant l'entrée aux personnes non autorisées. Cela garantit que seules les personnes autorisées peuvent entrer dans les zones sensibles ou restreintes, en conformité avec les consignes des clients.

La vidéo surveillance complète cette protection en fournissant une surveillance visuelle en temps réel des zones clés du site. En utilisant des caméras stratégiquement positionnées, les clients peuvent surveiller les activités sur le site, détecter toute intrusion ou comportement suspect, et vérifier visuellement l'identité des personnes accédant aux locaux.

Quant à la centrale d'alarme, elle agit comme le cœur du système de sécurité en surveillant en permanence les capteurs et en déclenchant des alarmes en cas de détection d'un événement indésirable, comme une intrusion ou un incendie. Les consignes des clients et leurs horaires d'activité peuvent être programmés dans la centrale d'alarme pour définir des actions spécifiques à prendre en fonction de la situation.

Sous certaines conditions préalablement établies par les clients, le télésurveilleur peut alors prendre des mesures appropriées, comme l'envoi d'un agent de sécurité sur place pour vérifier la situation et intervenir si nécessaire. Ces conditions sont généralement telles que le déclenchement d'une alarme sur la centrale (en dehors des heures d'activité), ce qui alertera le télésurveilleur. Il devra ainsi vérifier s'il y a présence humaine via la vidéo surveillance et. Cette coordination rapide entre les différents équipements permet de garantir une réponse rapide et efficace aux incidents de sécurité, réduisant ainsi les risques pour les biens et les personnes sur le site.

### 3.5) Préparations de tous ses équipements

Après avoir pris connaissances de ses équipements, j'ai eu pour tâche de préparer ces équipements pour que les techniciens aient que du « Plug and Play ». C'est-à-dire en ce qui concerne la vidéo protection je procède à toutes les modifications nécessaires, allant de l'installation de l'OS jusqu'à la création de l'utilisateur du télésurveilleur et sa configuration. Une fois toutes les étapes assimilées, j'ai mis à dispositions une documentation expliquant chaque étape de la configuration du serveur.

En ce qui concerne le contrôle d'accès, j'ajoute les informations nécessaires avec la numérotation des bureaux

Ce qui donne cela :

EQUIPEMENTS SALTO SUJET A PARAMETRAGE														
IQ - MAC ADDRESS	Act code	Localisation	#	#	XS4 - ID	Bureaux	#	XS4 - ID	Bureaux	#	XS4 - ID	Bureaux	CU - ID	NOM
00-0A-83-0A-92-7F	2978 6A40 E2A5	RO-Q-01	46	1	012805220000F1	1	46	01540F22000085	334	91			1	29 1C B7 7D
00-0A-83-0A-92-7B	2978 69E7 D9B5	RO-Q-02	47	2	012305220000FA	2	47	01540F22000089	335	92			2	29 1C AF 65
			48	3	012905220000FD	3	48	01590F2200008A	336	93			3	29 1C B1 78
00-0A-83-0A-92-77	2978 6718 85C0	R3-Q-03	49	4	01700F220000AE	4	49	01520F22000081	337	94			4	29 1C B5 7F
00-0A-83-0A-92-79	2978 680A 6E3E	R3-Q-04	50	5	01760F220000AD	5	50	014F0F2200009C	338	95			5	29 1C B6 7C
00-0A-83-0A-92-8C	2978 6E89 5765	R3-Q-05	51	6	01780F220000A8	6	51	01540F22000087	339	96			6	29 1C B6 7C
00-0A-83-0A-92-81	2978 68C5 3934	R3-Q-06	52	7	017C0F220000AF	7	52	01500F22000083	340	97			7	
00-0A-83-0A-92-90	2978 6F04 6E8F	R3-Q-07	53	8	01700F220000A5	8	53	01890422000031	341	98			8	
00-0A-83-0A-92-89	2978 6D4C 6F72	R3-Q-08	54	9	01750F220000A6	9	54	01E0422000032	342	99			9	
00-0A-83-0A-92-50	2944 CA51 D9FD	R3-Q-09	55	10	01730F220000A0	10	55	01E042200003D	343	100			10	
00-0A-83-0A-92-75	2978 66C7 5C93	R3-Q-10	56	11	01760F220000AC	11	56	01E8042200003D	344	101			11	
00-0A-83-0A-92-54	2944 CCA4 872B	R3-Q-11	57	12	017C0F220000AF	12	57	01E8042200003E	345	102			12	
00-0A-83-0A-92-5B	2944 CRC 202D	R3-Q-12	58	13	01740F220000A9	13	58	01E7042200003F	346	103			13	
00-0A-83-0A-92-56	2944 CD21 0AF1	R3-Q-13	59	14	01780F220000A7	14	59	01E2042200003A	347	104			14	
00-0A-83-0A-92-5C	2944 D06F D729	R3-Q-14	60	15	01740F220000A7	15	60	01E8042200003B	348	105			15	
00-0A-83-0A-92-5E	2944 D14B A46C	R3-Q-15	61	16	01C60E22000014	16	61	013605220000EF	349	106			16	
00-0A-83-0A-92-5F	2944 D2AF 588C	R3-Q-16	62	17	018F0E220000ED	17	62	013705220000EE	350	107			17	
00-0A-83-0A-92-59	2944 CDBF C13F	R3-Q-17	63	18	01720F220000A1	18	63	013405220000ED	351	108			18	
00-0A-83-0A-92-85	2978 6C3C A379	SPARE 1	65	20	01790F220000AA	20	64	013505220000EC	352	109			19	
00-0A-83-0A-92-52	2944 CBE2 BD7B	SPARE 3	66	21	010905220000DD	21	66	013205220000EB	354	111			21	
			67	22	010405220000DD	22	67	013305220000EA	355	112			22	
			68	23	010505220000DC	23	68	011095220000F7	356	113			23	
			69	24	010805220000DD	24	69	014F0522000096	357	114			24	
00-0A-83-0A-92-6E	2978 63CE 4D76	1	70	25	01E0422000037	25	70	1.48052E+12	358	115			25	
00-0A-83-0A-92-6A	2978 61D0 2908	2	71	26	01F10422000029	26	71	014A0522000093	359	116			26	
00-0A-83-0A-92-6C	2978 6295 6B87	3	72	27	01F00422000028	27	72	014B0522000097	360	117			27	
00-0A-83-0A-92-71	2978 6548 A0C3	4	73	28	01720F220000A1	28	73	0103052200003A	361	118			28	
00-0A-83-0A-92-70	2978 64CE 6E46	5	74	29	010105220000DB	29	74	01E4052200003D	362	119			29	
			75	30	010305220000DA	30	75	014D0522000094	363	120			30	
00-0A-83-0A-92-62	2978 56A FADD	CR+3	76	31	01FD0422000025	31	76	014B0522000092	364	121			31	
			77	32	01FE0422000026	32	77			122			32	
			78	33	011F0522000096	33	78			123			33	
			79	34	012805220000F2	34	79			124			34	
			80	35	0145052200009C	35	80			125			35	
			81	36	012D05220000F4	36	81			126			36	
			82	37	01F80522000021	37	82			127			37	
			83	38	01F3052200002A	38	83			128			38	
			84	39	01F2052200002B	39	84			129			39	
			85	40	01F00522000029	40	85			130			40	
			86	41	01E00522000035	41	86			131			41	
			87	42	01E6052200003F	42	87			132			42	
			88	43	01B80522000032	43	88			133			43	
			89	44	01B0052200003D	44	89			134			44	
			90	45	01550F22000086	45	90			135			45	

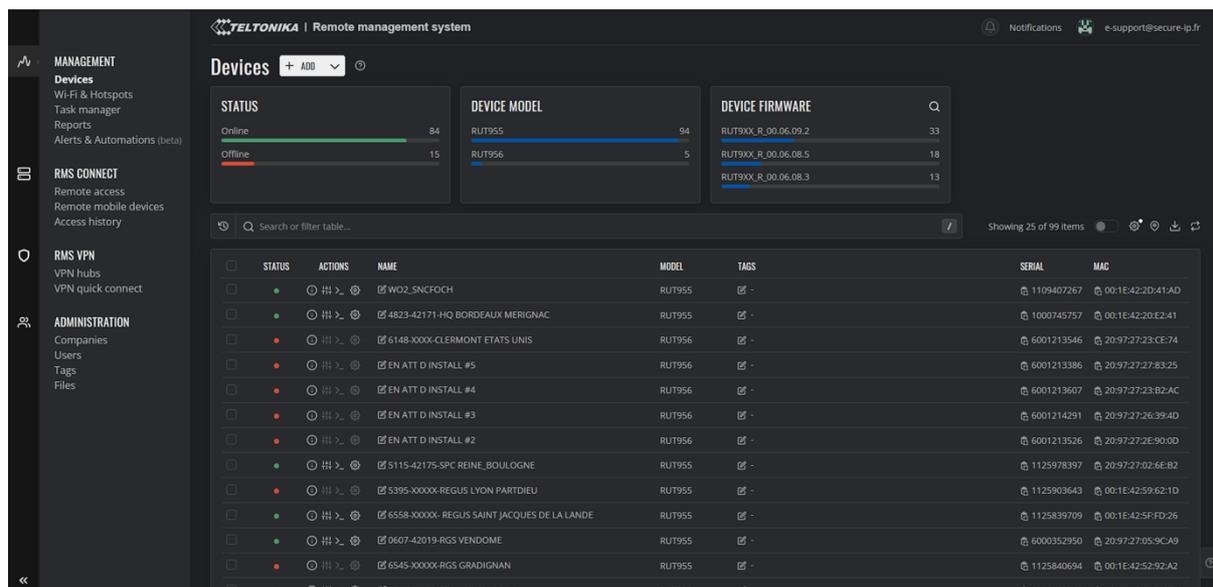
Pour ce qui est de la préparation des centrales Vanderbilt, nous avons décidés de ne plus les préparer en avance car cela est plus simple à préparer sur site en fonction de l'installations

### 3.6) Maintenance de ses équipement et améliorations

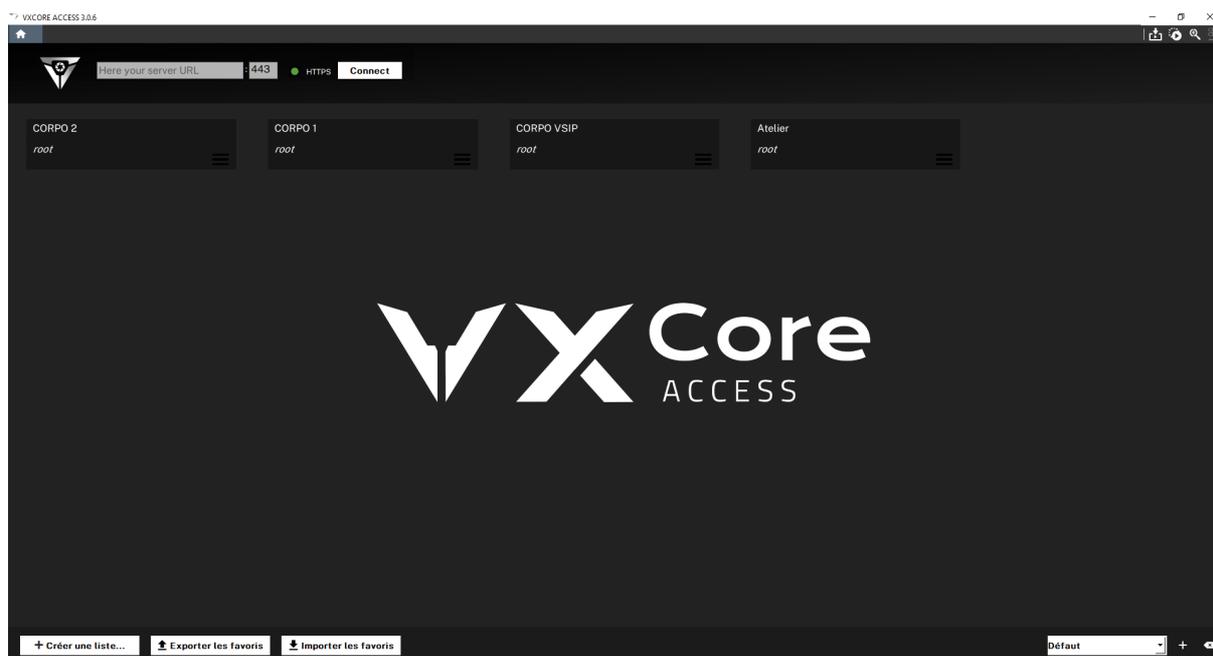
En fonctions de ticket ou même des mises a jours constructeurs, nous pouvons effectuer à distances la maintenance des équipements grâce à TeamViewer ou encore avec l'installations de Teltonika sur site ce qui nous permet d'avoir la main à distance sur divers équipement.

Serveur vidéo : Possibilité de connexion via le corporate depuis le software Vxaccess ou encore via le Teltonika depuis notre flotte sur [RMS](#).

RMS :



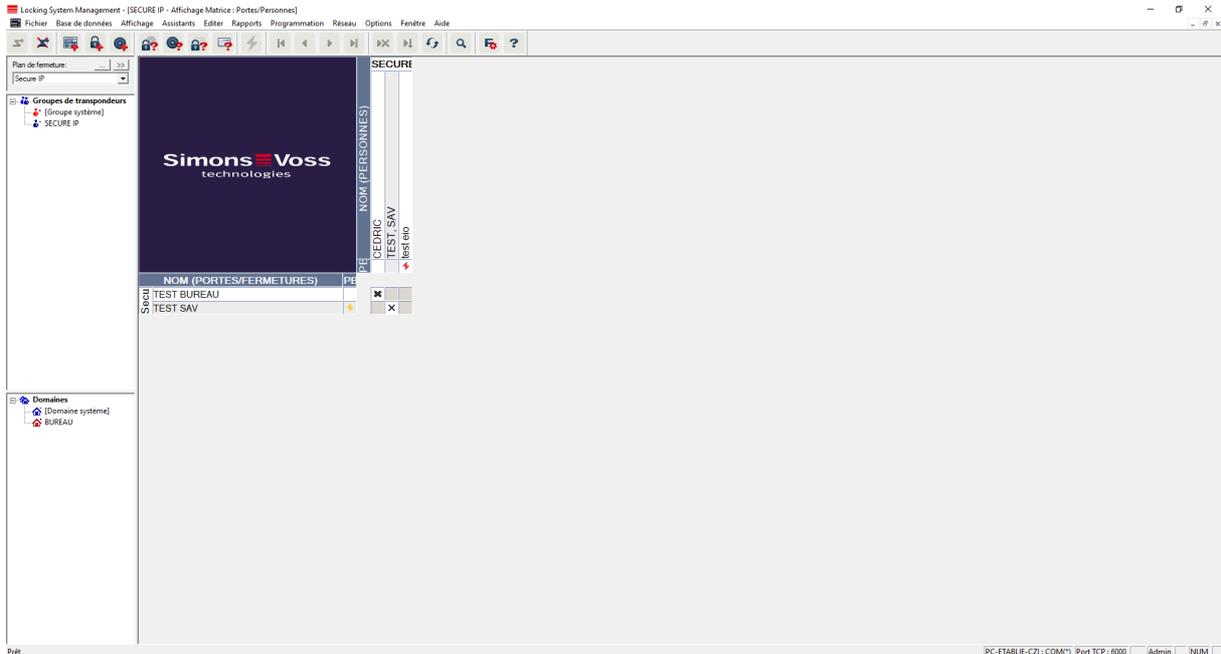
VxCore ACCESS :



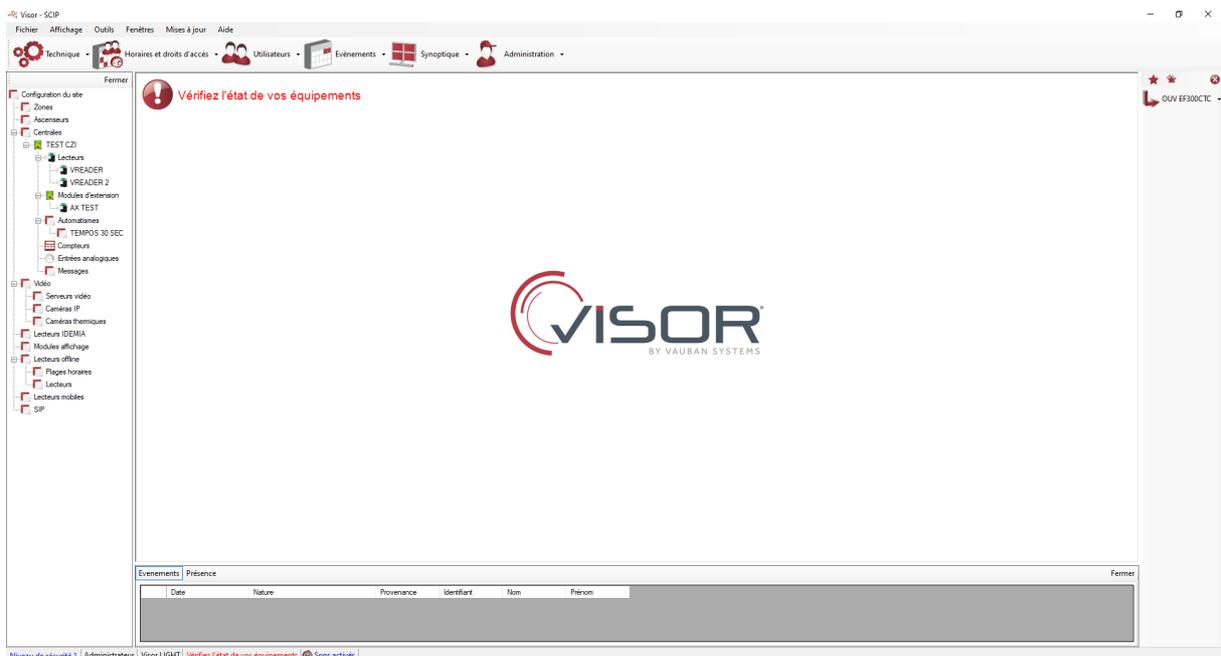
Contrôle d'accès : Possibilités différents suivant l'équipement utilisé :

Lsm et Visor qui utilisent du Simon Voss et Salto pro Access, fonctionnent grâce à une méthode de management du contrôle d'accès via un software et sera donc uniquement via TeamViewer sur le serveur du site concerné.

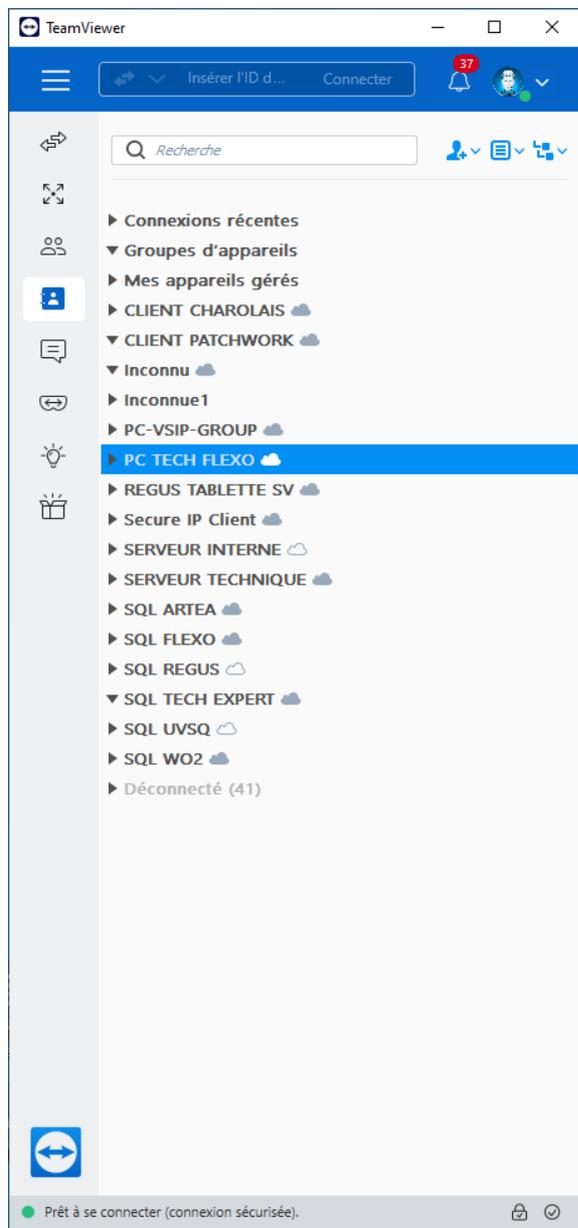
Lsm :



Visor :

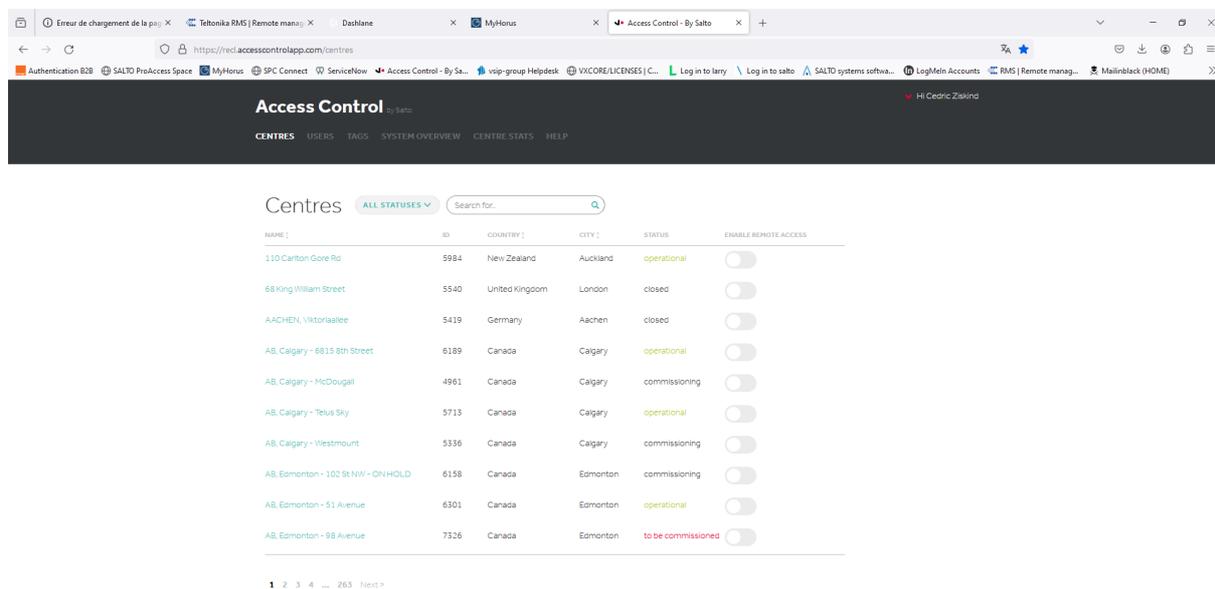


Liste TeamViewer :



Le reste du Salto (accès control et Ks) est directement héberger chez Salto et est accessible via leurs sites internet. Une fois connecter, tous les sites qui nous sont confier seront accessibles et mangeables.

### Access Control :



Centrale d'alarme : Est accessible via le site SpcConnect Pro ou via le Teltonika.

## 4) Collaboration et communication durant l'apprentissage

### 4.1) Reporting

Afin de mieux organiser mon temps, prévoir les tâches à faire la semaine suivante et Avoir une meilleure visibilité sur mon parcours professionnel au sein de Secure-IP J'envoyais un reporting chaque fin de semaine à mon maître de stage. Ce reporting contenait :

- Brève synthèse des réalisations de la semaine
- Prévisions d'activités pour la semaine suivante avec l'estimation de temps nécessaire
- 

### 4.2) Communication avec le maitre de stage

J'ai bénéficié d'un soutien précieux de la part de mon supérieur dans le cadre de mes projets professionnels. Il m'a confié des missions assorties de ressources pertinentes pour renforcer mes compétences. En outre, il m'a régulièrement suggéré des pistes d'amélioration et prodigué des conseils avisés. Son appui a été un facteur déterminant dans la réussite de mon parcours d'apprentissage.

Notre échange s'est principalement déroulé en présentiel, favorisant ainsi une communication directe et efficace.

#### 4.3) Communication avec d'autres collaborateurs

Pendant cet apprentissage, je me suis adressée à plusieurs collaborateurs afin de produire un travail de qualité et conforme aux normes et aux pratiques de l'entreprise. Notamment, j'ai échangé régulièrement avec nos techniciens concernant des points d'améliorations sur différentes solutions. Ses échanges se font principalement via conversations téléphonique, email ou physiquement, ce qui est plus rare.

## 5) Compétences acquises correspondant à l'épreuve E4 du BTS

### 5.1) Gérer le patrimoine informatique

Sur le serveur vidéo il est possible de faire des backups de celui sur un FTP :

VXCORE ACCESS 3.0.3

Regus Corporate II

6062-42260-HQ NORDPONT MONTPARNASSE

6062-42260-HQ NORDPONT MONTPARNASSE / 2023-05-30 09:53:49 / Network:WAN / root

### Maintenance / Sauvegarde et restauration

Sauvegarde des paramètres par le réseau

Exporter les paramètres

Restauration des paramètres par le réseau

(\*) : Attention, pour effectuer cette action, vous devez activer le mode de maintenance.

### Exportation des paramètres systèmes par S/FTP

Protocole: FTP

Serveur: [ ]

Port: [ ]

Utilisateur: [ ]

Mot de passe: [ ]

Répertoire distant: Regus-NORD-PONT

Mode passif (FTP)

Appliquer Tester l'envoi des paramètres

Last Backup/Upload : 2023-05-30 03:00:10

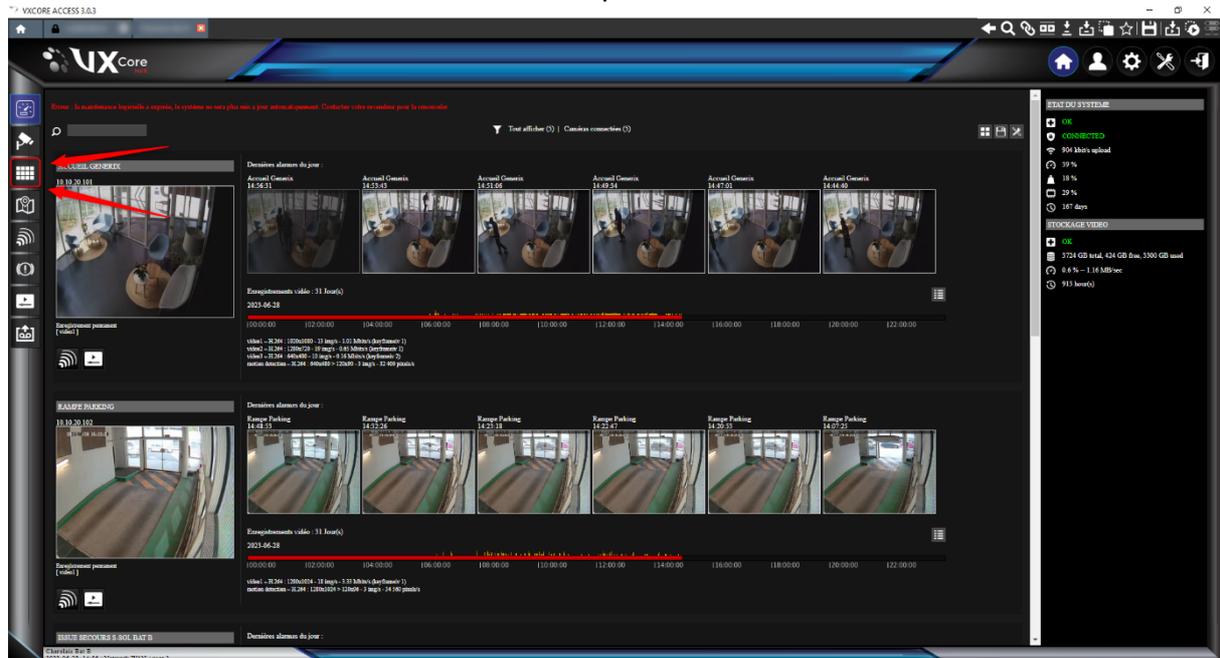
Try to Send /tmp/VXCORE-CONFIG\_20230530030009.veox (11K) to FTP server ftpperso.free.fr ... 1/5

```
>>> Net:FTP(3.11)
>>> Exporter(5.74)
>>> Net:Cmnd(3.11)
>>> IO:Socket-SSL(2.069)
```

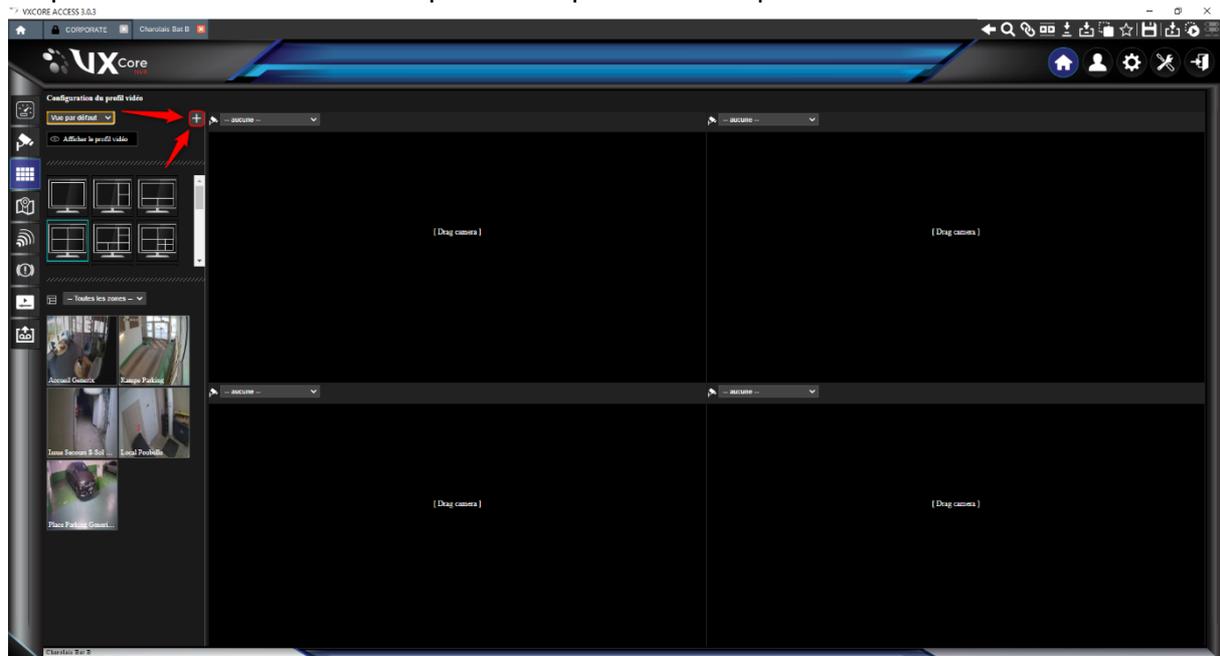
## 5.2) Répondre aux incidents et aux demandes d'assistances et d'évolutions

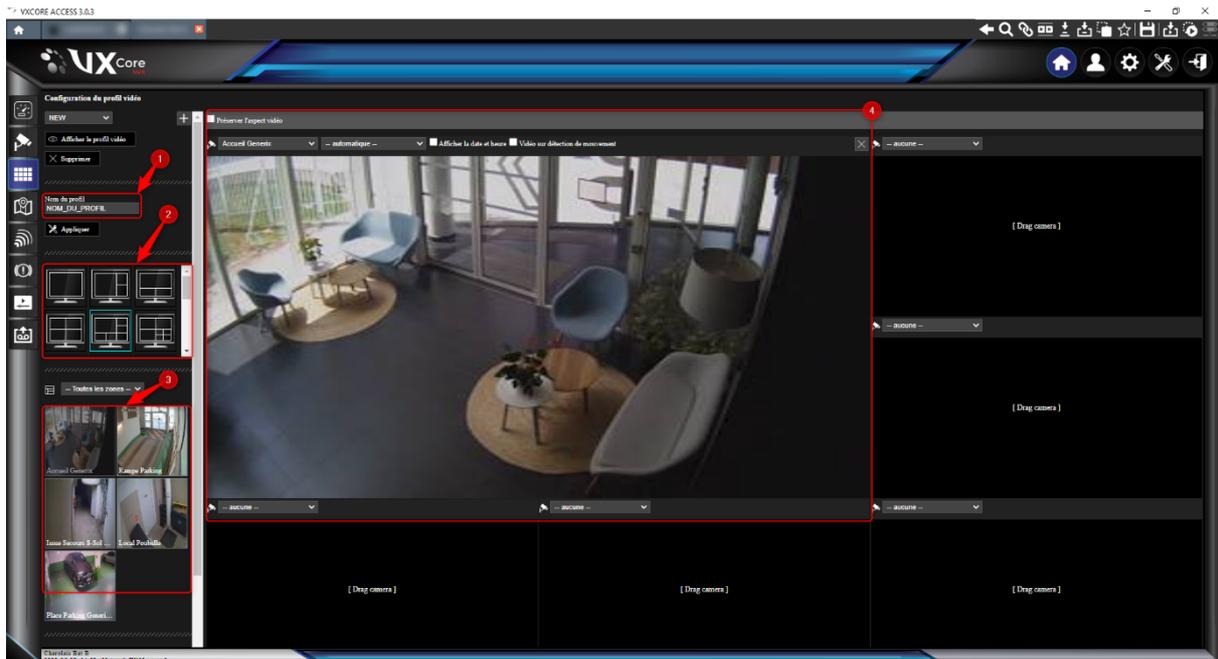
Un client avec lequel nous n'avons pas de contrat de maintenance a ouvert un ticket pour s'avoir comment créer un profil vidéo sur Vxcore. J'ai donc rédigé un document répondant à leur demande :

Connectez vous sur votre serveur vidéo et cliquez sur l'icône multi-vues.

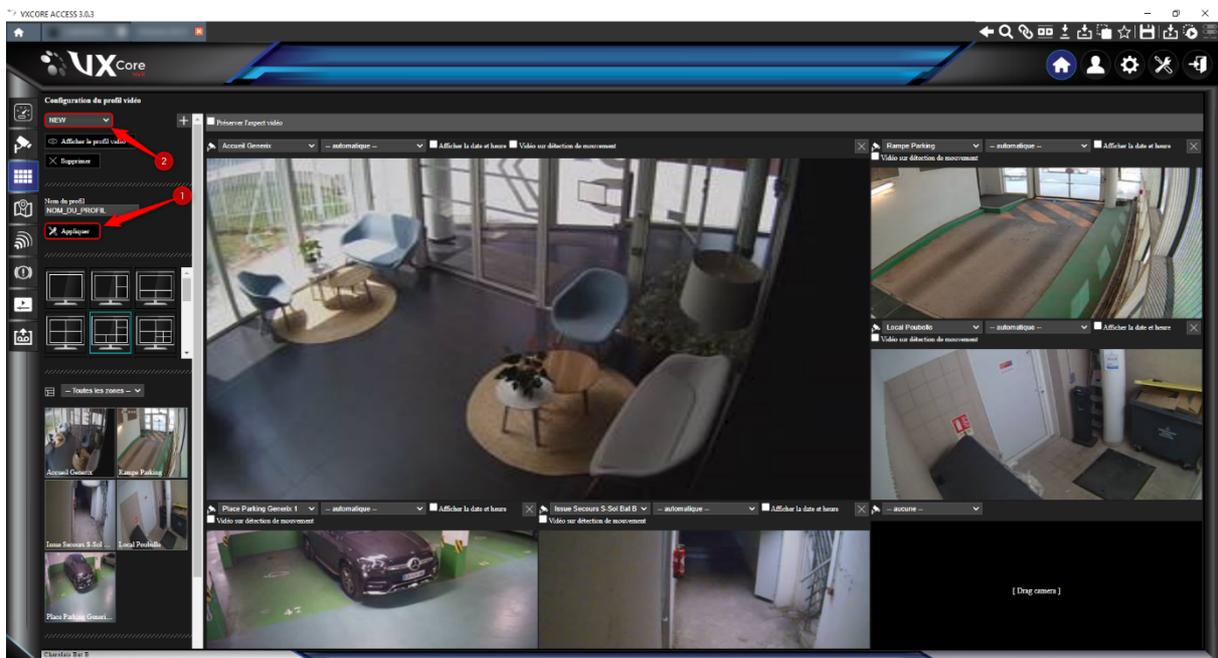


Cliquez sur le + à droite de vues par défaut pour créer un profil de vision.





- 1) Tapez le nom du profil que vous souhaitez
- 2) Sélectionnez la vision qui vous convient (ici on choisit un profil pouvant accepter 5 caméras).
- 3) Cliquez sur une image pour la retransmettre dans la partie visualisation.
- 4) L'image sur laquelle vous avez cliqué est dans la partie visualisation



- 1) Une fois le profil terminé enregistrez le en appuyant sur le bouton appliquer juste en dessous du nom du profil.
- 2) Vous pouvez sélectionner différentes vues au-dessus du bouton Afficher le profil vidéo.

### 5.3) Mettre à disposition des utilisateurs un service informatique

Afin de voir la finalité des solutions préparé, mes supérieur mon permis de participer à la pose de nos équipements sur site. Pour ma part j'ai installé les IQ et Caméras sur l'ensemble du site, mais aussi l'ensemble de nos équipements dans la baie informatique, c'est-à-dire serveur vidéo, switch et Teltonika.



## Conclusion

Mon expérience en alternance chez Secure-IP, une PME spécialisée dans la vidéo protection et le contrôle d'accès, a été enrichissante à bien des égards. Pendant ces deux années, j'ai eu l'opportunité d'acquérir une expertise pratique dans le domaine de la sécurité physique des infrastructures, en participant à la mise en place, à la configuration et à la maintenance des systèmes de sécurité. Cette expérience m'a permis de développer des compétences techniques solides et une compréhension approfondie des technologies utilisées dans ce secteur.

En tant qu'aspirant à une carrière dans la cybersécurité offensive, cette expérience chez Secure-IP m'a également apporté des avantages sur le plan professionnel et personnel. Professionnellement, j'ai pu développer des compétences essentielles telles que l'analyse des vulnérabilités, la gestion des incidents de sécurité et la compréhension des risques liés aux systèmes informatiques. Sur le plan personnel, j'ai renforcé des qualités telles que la rigueur, la responsabilité et la résolution de problèmes, ainsi que des compétences interpersonnelles précieuses comme la communication efficace et la collaboration en équipe.

En combinant cette expérience avec une formation continue et un engagement dans le domaine de la cybersécurité, je suis convaincu que je suis bien positionné pour réaliser mes aspirations professionnelles et atteindre mes objectifs dans ce domaine en constante évolution. Je suis reconnaissant envers Secure-IP pour cette opportunité et je suis impatient de mettre à profit les compétences et les connaissances que j'ai acquises dans ma future carrière professionnelle.

## Glossaire technique

**IQ 21** : L'IQ 2.0 utilise la connectivité cellulaire 2G, 3G et 4G pour communiquer avec le Cloud SALTO. Également disponible en version Wi-Fi ou POE et toujours disponible via une connexion Ethernet. L'IQ 2.0 communique avec les points d'accès SALTO KS via ZigBee/Bluetooth.

**Software** : Un logiciel (ou software en anglais) désigne un ensemble de programmes informatiques, de données et de procédures qui permettent à un ordinateur d'effectuer des tâches spécifiques. Il peut prendre différentes formes, telles que des applications, des systèmes d'exploitation, des jeux, des utilitaires, etc. Les logiciels sont conçus pour exécuter des fonctions précises, telles que le traitement de texte, la gestion des bases de données, la navigation sur Internet, etc., en utilisant les ressources matérielles de l'ordinateur, telles que le processeur, la mémoire et le stockage.

**OS** : Un système d'exploitation (OS), également appelé système opérationnel, est un ensemble de logiciels qui contrôle les ressources matérielles et permet l'exécution d'autres programmes sur un ordinateur ou un appareil informatique. L'OS assure des fonctions fondamentales telles que la gestion des fichiers, la communication avec les périphériques, la gestion de la mémoire, la planification des tâches et l'interface utilisateur. Il sert d'intermédiaire entre les utilisateurs et le matériel informatique, facilitant ainsi l'utilisation de l'ordinateur et permettant l'exécution de diverses applications et programmes. Exemples d'OS populaires incluent Windows, macOS, Linux, Android et iOS.

**Plug and Play** :

Plug and Play (PnP) est une technologie informatique qui permet à un périphérique matériel d'être automatiquement détecté et configuré par un système d'exploitation sans nécessiter d'intervention manuelle de l'utilisateur. Lorsqu'un périphérique Plug and Play est connecté à un ordinateur, le système d'exploitation reconnaît automatiquement le périphérique, charge les pilotes nécessaires et configure les paramètres appropriés pour son fonctionnement. Cette technologie simplifie grandement l'installation et l'utilisation de périphériques matériels tels que les claviers, les souris, les imprimantes, les scanners, les périphériques de stockage, etc., offrant ainsi une expérience utilisateur plus conviviale et pratique.

**Teltonika RUT955** : C'est un routeur(4G) industriel conçu pour fournir une connectivité Internet fiable dans des environnements professionnels et industriels. Il est équipé de plusieurs ports Ethernet, de connexions sans fil Wi-Fi, ainsi que de fonctionnalités avancées telles que le VPN, la gestion des réseaux virtuels privés, la sauvegarde automatique de la connexion Internet, la prise en charge de cartes SIM redondantes. Le RUT955 est conçu pour offrir une connectivité haut débit sécurisée et stable dans les applications industrielles, les sites distants, les véhicules, les installations temporaires, etc.