



# RAPPORT DE STAGE

---

Lucas De Oliveira  
2025

Tuteur pédagogique :  
Frank POLI

# Remerciement

Je souhaite exprimer ma profonde reconnaissance à ceux qui m'ont accompagné et conseillé durant mon stage, que ce soit pour développer mes compétences ou améliorer mes relations sociales au travail.

Je remercie dans un premier temps, François DELZANT pour l'opportunité qu'il m'a offerte et la confiance qu'il m'a accordé afin de rejoindre le pôle Cybersécurité du groupe Crédit Agricole S.A.

Je remercie fortement mon tuteur de stage Frank POLI pour sa bienveillance et son accueil dans ce nouvel environnement, ainsi que son envie sincère que je me plaise et apprenne de nouvelles choses.

Je remercie également Thomas BRZYCHEY, Christine BOVE, Alain STEPHAN, Céline DOZIERES, Bassem DERBAL, Antonio DEL RIO MENDEZ, Alexis-Isidore DESHAIES, Olivier CHRISTOPHE, Samyr CHAKHAB, Gilles NERONDAT, David MAUCOURT, Elise NASCIET, Tristan DAIGLE, Henry NDEPO, William DESMOLIN, Loïc LEFORT et Catherine FOURQUIER pour avoir pris de leur temps pour m'expliquer leur mission, de leur disponibilité lorsque j'avais des questions et de m'avoir partagé leur savoir durant ces 5 semaines.

Enfin, je remercie Véronique JUDAIQUE ma superviseuse qui a été particulièrement bienveillant et disponible.

# Lexique

**RSSI/CISO (Responsable de la Sécurité des Systèmes d'Information)** : il définit et développe la politique de sécurité de l'information de son entreprise. Il est garant de sa mise en œuvre et en assure le suivi. Il protège l'entreprise des risques liés aux cyberattaques. Il assure aussi des projets comme les politiques de sécurité interne au niveau des employés.

**ODrive** : c'est un éditeur de logiciels dont le cœur de métier est la protection de la donnée sensible pour les entreprises. La société propose une suite collaborative en SaaS comprenant des solutions cloud : partage de fichiers, conférence sécurisée et signature électronique.

**DICP (Disponibilité, Intégrité, Confidentialité et Preuve)** : critères de classification des biens.

**DNS (Domain Name System)** : système permettant d'établir une correspondance entre un nom de domaine et une adresse IP et, plus généralement, de trouver une information à partir d'un nom de domaine.

**AD (Active Directory)** : est une base de données et un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources réseau dont ils ont besoin pour mener à bien leurs missions.

**API (Application Programming Interface)** : une interface de programmation d'application est un ensemble normalisé de classes, de méthodes, de fonctions et de constantes qui sert de façade par laquelle un logiciel offre des services à d'autres logiciels.

**SOC (Security Operations Center)** : c'est une unité de surveillance dédiée aux incidents de sécurité (approche industrielle) intervenant lorsqu'une concordance de signaux permet de soupçonner ou d'attester une activité informatique malveillante au sein d'un système d'information. Leur mission est de détecter, analyser, réagir, signaler, prévenir et remédier en cas d'incident de sécurité. Chaque production informatique est supervisée par un SOC.

**CERT (Computer Emergency Response Team)** : cette unité centralise les demandes d'assurances suite à des attaques, traite les alertes, établit et maintient une base de données des vulnérabilités, assure la prévention par la diffusion d'informations sur les précautions à prendre.

**SIEM (Security Information and Event Management)** : c'est une base de données pour le SOC qui permet de surveiller, détecter et alerter sur tout événement ou incident lié à la sécurité du système d'information avant toute perturbation des activités de l'organisation. Il fournit une vision globale et centralisée de la posture de sécurité d'une infrastructure IT.

**WAF (Web Application Firewall)** : permet de filtrer les demandes d'accès émanant d'internet vers les applications internes.

**SaaS (Software as a Service)** : modèle de distribution dans le cloud de logiciel au sein duquel un fournisseur tiers héberge les applications et les rend disponibles pour ses clients par l'intermédiaire d'internet.

**IaaS (Infrastructure as a Service)** : modèle de cloud computing destiné aux entreprises où : l'entreprise gère le middleware des serveurs, et surtout les logiciels applicatifs ; le fournisseur cloud gère le matériel serveur, les couches de virtualisation, le stockage, les réseaux.

**TLP (Traffic Light Protocol)** : niveau de sécurité selon quatre couleurs : le rouge, l'ambre + le vert + le blanc.

**IOC (Indicateur of Compromise)** : preuve et indices d'une fuite de donnée.

**Analyse Forensic** : sert à investiguer un système d'information après une cyberattaque pour savoir ce qu'il s'est passé et établir des conclusions.

**Supply Chain (ou chaîne d'approvisionnement)** : regroupe l'ensemble des fournisseurs, partenaires, clients et ressources impliqués dans la conception, la production et la distribution d'un produit ou d'un service.

**AES (Advanced Encryption Standard)** : est une norme ou spécification de chiffrement comme RSA, DES, ... C'est un chiffrement par bloc, le nombre de blocs est indiqué par le numéro : AES-128, AES-192 ou encore AES-256. C'est un chiffrement symétrique une même clé permet de chiffrer et de déchiffrer un contenu.

**PGP** (Pretty Good Privacy) = chiffre des e-mails ou des fichiers, pour les rendre lisibles par les seules personnes autorisées.

**RFC** (Request For Comments) = ce sont des documents publics qui définissent les normes techniques sur lesquelles s'appuient le réseau Internet.

**SSL/TLS** (Secure Socket Layer/Transport Layer Security) = correspond à un ensemble de protocoles de sécurisation des échanges. Utilisé nativement sur la quasi-totalité des systèmes, il permet de garantir la confidentialité, l'intégrité et l'authentification des échanges.

**HTTPS** = sécurisé grâce à l'utilisation de SSL/TLS (les données transmises entre un navigateur Web et un site Web restent privées et protégées).

**Proxy** = un serveur proxy (appelé aussi serveur mandataire en français) est, dans le cadre des réseaux et d'internet, est une machine qui fait l'intermédiaire entre internet et votre matériel (ordinateur, smartphone, tablette...).

**Attack Heartbleed** = Le bug Heartbleed est une grave vulnérabilité dans la bibliothèque logicielle cryptographique populaire OpenSSL. Cette faiblesse permet de voler les informations protégées, dans des conditions normales, par le cryptage SSL/TLS.

**SSO** (Single Sign-On) : est un service d'authentification de session et d'utilisateur qui permet à un utilisateur d'utiliser un ensemble d'informations d'identification (par exemple, nom et mot de passe) pour accéder à plusieurs applications.

**KPI** (Key Performance Indicator) = indicateur utilisé pour l'aide à la décision dans les organisations.

**KRI** (Key Risk Indicators) = mesure utilisée en gestion pour indiquer le degré de risque d'une activité.

**Bug Bounty** = ce programme, mis en place en partenariat avec YesWeHack, vise à renforcer la sécurité de FranceConnect en encourageant les hackers éthiques à signaler les failles de sécurité qu'ils pourraient identifier.

**OSINT** (Open Source Intelligence) = Il s'agit d'une information accessible à tous et non classifiée. L'Open Source Intelligence est un élément fondamental pour les opérations de renseignements.

# Sommaire

Remerciement .....	2
Lexique.....	3
Sommaire.....	6
Introduction .....	7
I.    L’entreprise du Crédit Agricole .....	8
1.    Présentation du groupe Crédit Agricole.....	8
2.    Le pôle CYG .....	9
II.    Les différentes équipes .....	11
1.    Cadre Normatif Cyber et SSI, et Coordination réseau .....	11
1.1.    Pôle VPS (Veille, Politique et Standard) .....	13
1.2.    Pôle Avis SSI (Sécurité et Risques des Systèmes d’Information) .....	14
2.    Red Team .....	15
3.    Evaluation et contrôle .....	18
4.    CISO du Crédit Agricole SA .....	25
5.    Risques IT .....	28
6.    Activités Transverses.....	33
Conclusion.....	34

# Introduction

Afin d'avoir une vue globale de la cybersécurité et de son importance, j'ai décidé de faire un stage au sein d'une des plus grandes banques françaises, le Crédit Agricole. En effet, un groupe d'importance vitale pour la France implique des contraintes et des sanctions beaucoup plus importantes, ce qui m'a permis de m'immerger dans les meilleures pratiques de cybersécurité.

Mon stage de 5 semaines s'est déroulé au sein du département Cybersécurité Groupe (CYG) du Crédit Agricole, une des plus grandes banques françaises et la dixième banque mondiale en termes d'actifs.

Ce dont j'avais vraiment besoin en tant que stagiaire, c'était de voir le panorama des possibilités de la cybersécurité pour ne pas m'enfermer dans un sujet. Par ailleurs, je ne pense pas qu'il soit possible d'être bon dans un domaine technique ou managérial, sans comprendre les objectifs et les besoins de ses collaborateurs, particulièrement dans la cybersécurité. Chaque équipe dépend des autres pôles, et comprendre sa véritable place au sein du groupe permet de mieux collaborer et d'améliorer ensemble les défenses de l'entreprise.

Ce rapport va présenter les différents pôles dans lequel j'ai été et les différentes missions que j'ai pu réaliser tout au long de ce stage.

# I. L'entreprise du Crédit Agricole

## 1. Présentation du groupe Crédit Agricole

Le Crédit Agricole est une institution financière française fondée à la fin du XIXe siècle pour soutenir les agriculteurs français. Depuis sa création, le Crédit Agricole a progressivement élargi ses activités pour devenir un acteur clé dans les services bancaires et financiers, offrant aujourd'hui une vaste gamme de services financiers à l'échelle internationale.



Le Groupe Crédit Agricole se distingue par son modèle unique de banque coopérative et mutualiste, possédant le plus grand réseau de banques coopératives et mutualistes au monde. En France, ce réseau comprend trente-neuf caisses régionales autonomes qui opèrent localement tout en bénéficiant de la solidarité et des ressources du groupe et de nombreuses filiales.

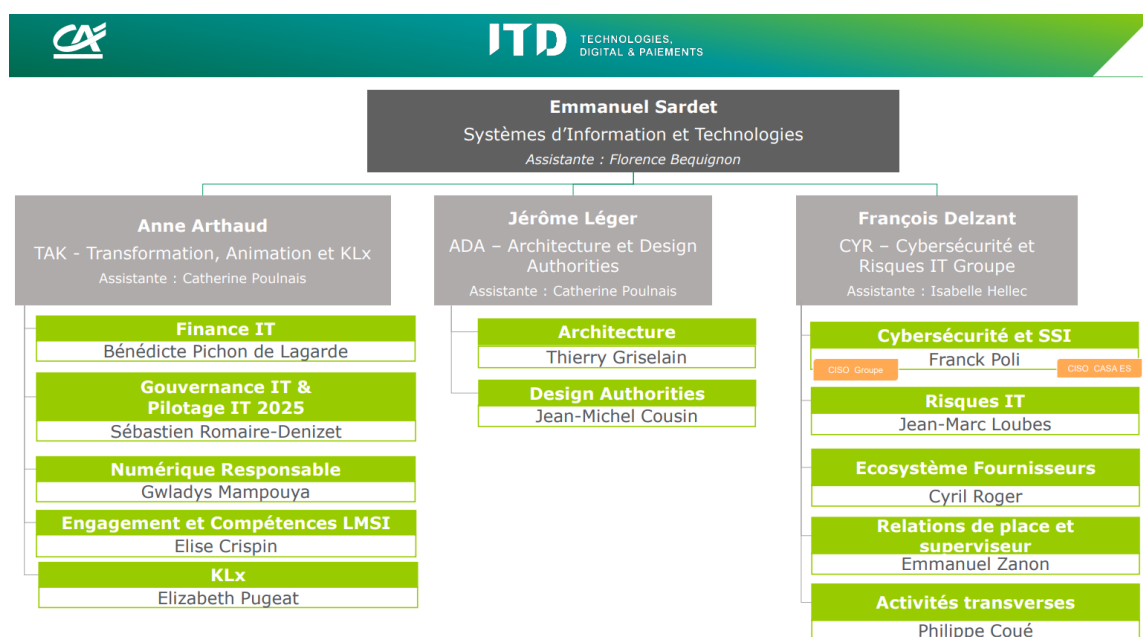
En 2024, le Crédit Agricole se classe comme la neuvième plus grande banque au monde en termes d'actifs, et la deuxième plus grande banque française. Le Groupe est le premier financeur de l'économie française, leader de la banque de proximité en Europe, premier gestionnaire d'actifs européen, premier bancassureur en Europe et troisième acteur européen en financement de projets.



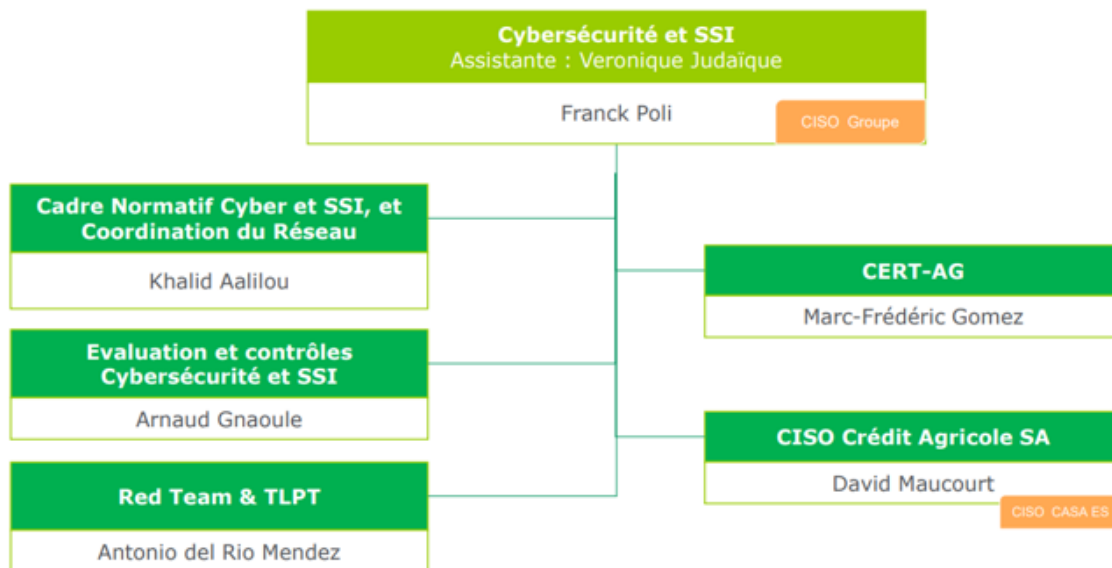
Malgré la mise en place de CA-GIP (Group Infrastructure Platform) et la centralisation des infrastructures informatiques du Groupe, Il est important de fédérer les entités autour d'une stratégie de sécurité unifiée. Également ils investissent 5,5 milliards d'euros dans l'informatique chaque année

## 2. Le pôle CYG

Conscient de ce défi, le Crédit Agricole a mis en place un pôle dédié à la cybersécurité, Cybersécurité Groupe communément appelé CYG. Ce pôle, présent au sein de l'entité mère du Crédit Agricole à savoir Crédit Agricole S.A. (CA-SA) est placé sous la responsabilité directe du CISO Groupe. C'est dans ce pôle que j'ai pu évoluer durant mon stage et qui m'a permis d'observer de près les enjeux cruciaux de la cybersécurité au sein d'une entreprise d'importance vitale pour la France.



Le défi majeur de l'entreprise réside dans la nécessité de maintenir une stratégie de sécurité cohérente malgré la dispersion de ses entités. Chaque membre du groupe possède ses propres systèmes informatiques, ce qui rend complexe la mise en place d'une approche cohérente en matière de cybersécurité. La mission principale de CYG consiste à élaborer et à mettre en place la stratégie de cybersécurité pour toute l'entreprise, assurant ainsi sa résistance.



Au sein de ce pôle, j'ai été affecté au CYR dans le service de Frank Poli où j'ai pu intégrer les différentes équipes du groupe Cybersécurité et SSI.

À présent je vais présenter chaque équipe où j'ai été affecté.

## II. Les différentes équipes

### 1. Cadre Normatif Cyber et SSI, et Coordination réseau



J'ai passé mes quatre premiers jours dans cette équipe.

#### Leur mission :

- Accompagner les CISO dès leur prise de poste, animer la communauté des acteurs de la SSI (Cercle des CISO, Libres Antennes, ...) et favoriser le partage de connaissances et bonnes pratiques.
- Apporter des réponses adaptées aux questions de sécurité des systèmes que nous posent les entreprises du groupe
- Donner un avis sécurité sur les projets transverses, stratégiques et sur les solutions cloud
- Réaliser des études transverses techniques sur la sécurité informatique du Groupe, formaliser les standards et effectuer une animation autour de la veille technologique.

#### Piloter et contrôler le risque SSI



Une équipe centrale de 50 collaborateurs  
dédiée à la gouvernance et au pilotage des risques liés à la sécurité du SI du Groupe au sein de Crédit Agricole SA

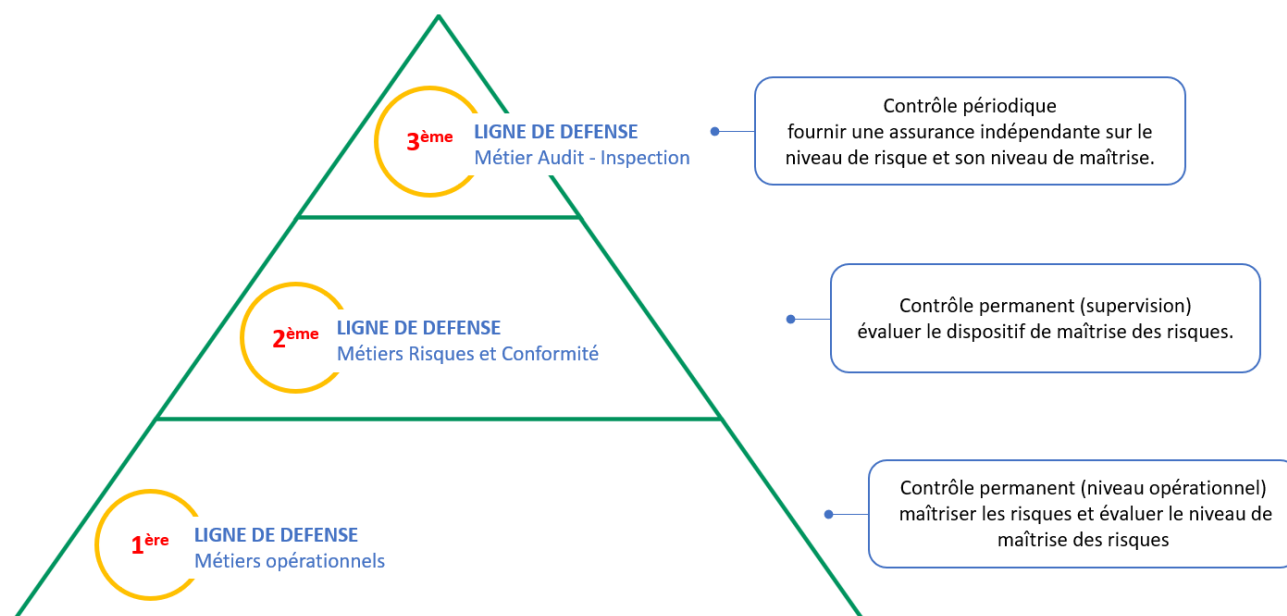


Un réseau de DSI, CISO et de RSI  
pour évaluer et maîtriser les risques spécifiques à chaque entité, mettre en œuvre et contrôler l'efficacité des dispositifs de sécurité locaux

Cette équipe dirige 5 secteurs :



Elle est située à la première ligne de défense



Il utilise un outil d'analyse de risque **MESARI**



## La méthode MESARI

Méthode Simplifiée d'Analyse de Risques de l'Information interne au Crédit Agricole.

La démarche d'analyse de risque MESARI est une démarche normée qui contribue à l'évaluation des risques pesant sur les systèmes d'information.

Elle sert pour l'analyse de risque et s'appuie sur la norme ISO 27 005.

### 1.1. Pôle VPS (Veille, Politique et Standard)

Dans l'équipe coordination et réseau il y a deux personnes qui s'occupe de ce pôle. (Alain et Céline)

#### Ils ont quatre missions :

- Développer la veille SSI
- Contribuer au cadre normatif SSI du groupe
- Apporter une expertise SSI dans les projets
- Animations transverses

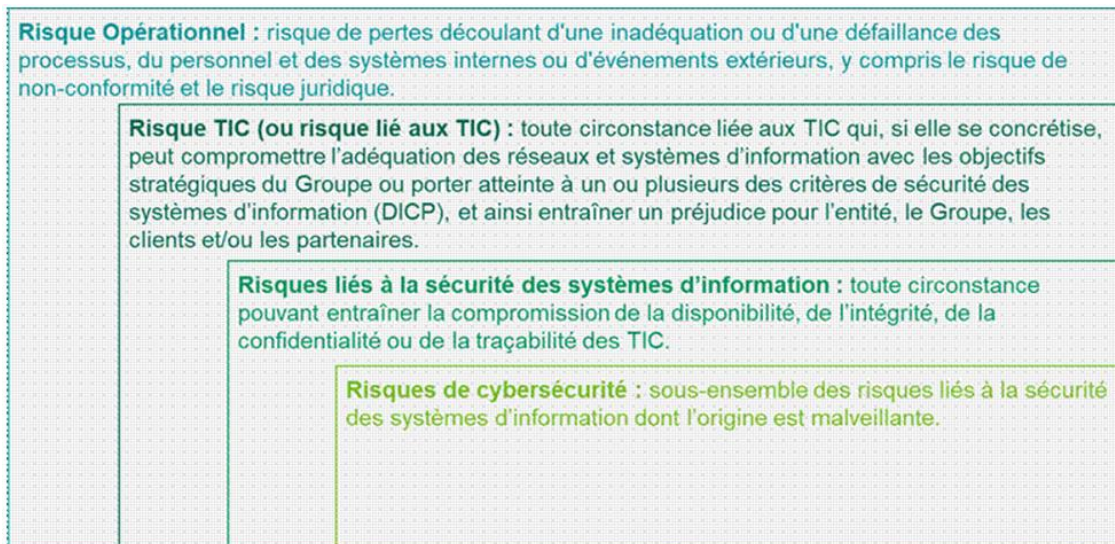
Ils doivent adapter le cadre normatif SSI aux évolutions des risques cyber et des technologies et apporter des éclairages sur les tendances innovantes en SSI.

Ils sont sous la réglementation DORA.



Le **Digital Operational Resilience Act (DORA)** est un règlement (n°2022/2554) adopté par l'Union européenne en décembre 2022 pour encadrer la cybersécurité des entités financières, telles que les banques et les établissements de crédit.

L'objectif final est de **maintenir la continuité opérationnelle** des services financiers au sein de l'Union européenne, même en cas de perturbations, d'incidents ou d'attaques. DORA marque **un changement de paradigme, le passage d'une vision défensive de la sécurité à une résilience globale** du secteur financier. Il ne s'agit plus seulement de se défendre, mais bien de résister.



## 1.2. Pôle Avis SSI (Sécurité et Risques des Systèmes d'Information)

Dans l'équipe coordination et réseau il y a qu'une seule personne qui s'occupe de ce pôle. (Bassem)

### Ces missions :

- Faire des dérogations (analyser les règles et remonter l'info)
- S'occuper du comité NAP (Nouvelle Activité Nouveau Produit)

### Outil utilisé dans la consolidation des avis SSI :



## 2. Red Team



J'ai passé mes quatre prochains jours dans cette équipe.

### Qu'est-ce que la Red Team ?

Une Red Team est une équipe de hackers éthiques. Ils sont experts dans la cybersécurité et des méthodes d'attaques des pirates malveillants. Ce groupe intervient en toute légalité auprès d'une entreprise ou une organisation pour tester la sécurité informatique. Considérée comme une véritable armée, elle génère des attaques réelles sur les systèmes, tel que pourraient le faire de vrais hackers.

#### Leurs missions :

- R & D / Veille
- Mener des missions en binôme

Detection → Intrusion test (ou physique)

Reaction → Blue Team

Process → Gérer les habilitations

#### Suivi et rapport :

Audit de 15j

Missions en 3 mois

Tout ne leur ai pas permis

- Pas de dégradation du niveau de sécurité
- Remonter immédiatement la vulnérabilité

### Les étapes en pentesters :

- 1) Reconnaissance (service en ligne, implantation physique, liste des employés, offres d'emploi)
- 2) Intrusion
- 3) Post Exploitation
- 4) Déplacement latéral
- 5) Atteinte des objectifs

### **Objectifs (→ accéder à la donnée)**

- Accès à la base de données (XSS, remote)
- Compte d'un utilisateur de l'application
- Extraction de la base faite par un utilisateur
- Accès au serveur hébergement l'application

### Outil qu'il utilise

- Google Gruyère
- Burp
- Hashcat
- Caddy
- Symantec
- Evilginx (pour le phishing)

### **Attaque en physique :**

- Implant (installation d'un mini-pc entre une photocopieuse et le SI de l'entreprise)
- Clé USB (pour le programmer comme une entrée clavier et installer un logiciel malveillant)

### Compétences :

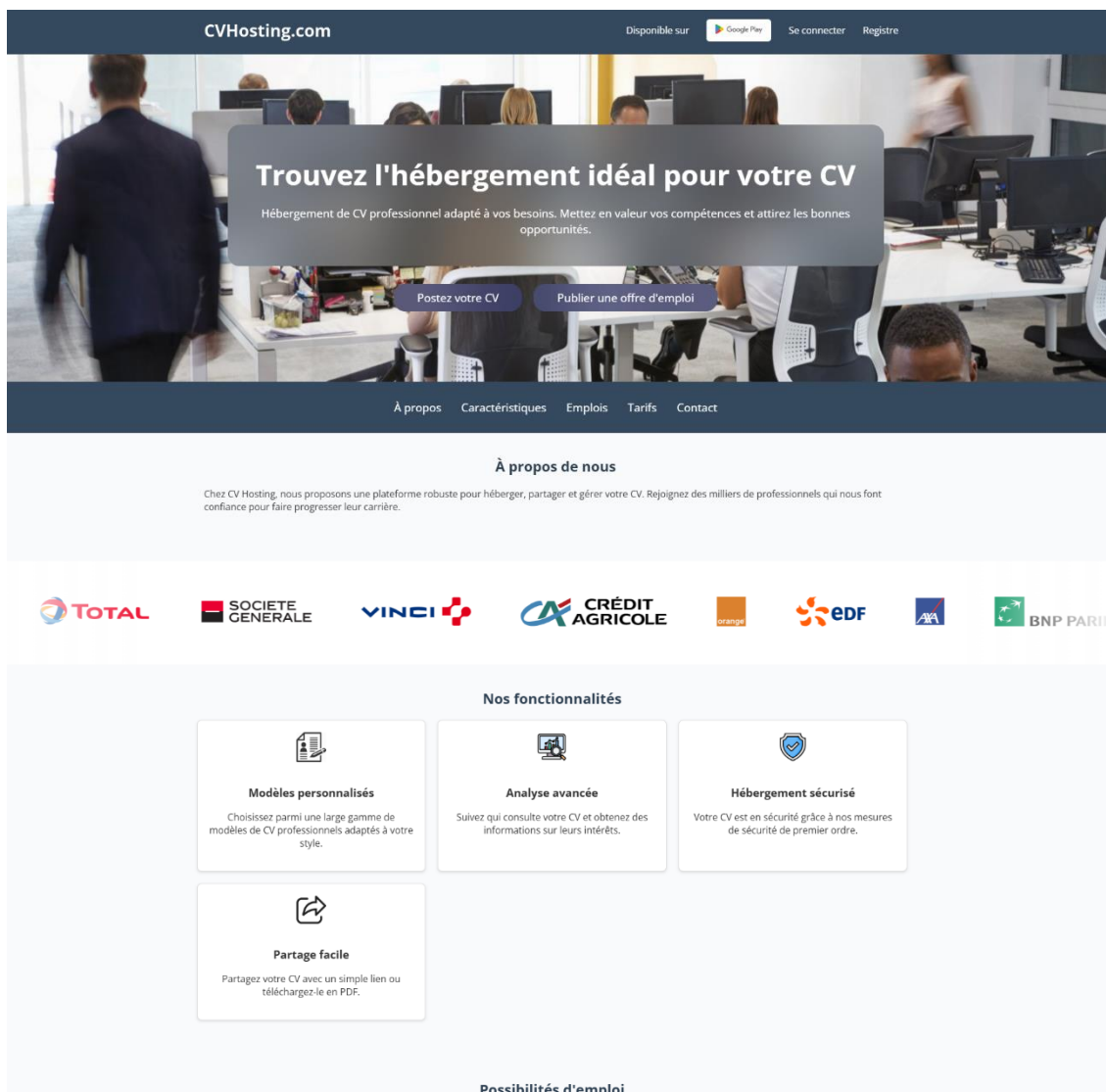
- Réseau
- Système (Unix et Windows)
- Architecture : web, PKI, AD, virtualisation
- Développement et scripting (powershell, python, C++, ...)
- Une expérience préalable dans la sécurité informatique



Documentation : OWASP qui regroupe le top 10 des vulnérabilités sur le web



J'ai pu réaliser un site vitrine de phishing pour leur équipe



### 3. Evaluation et contrôle

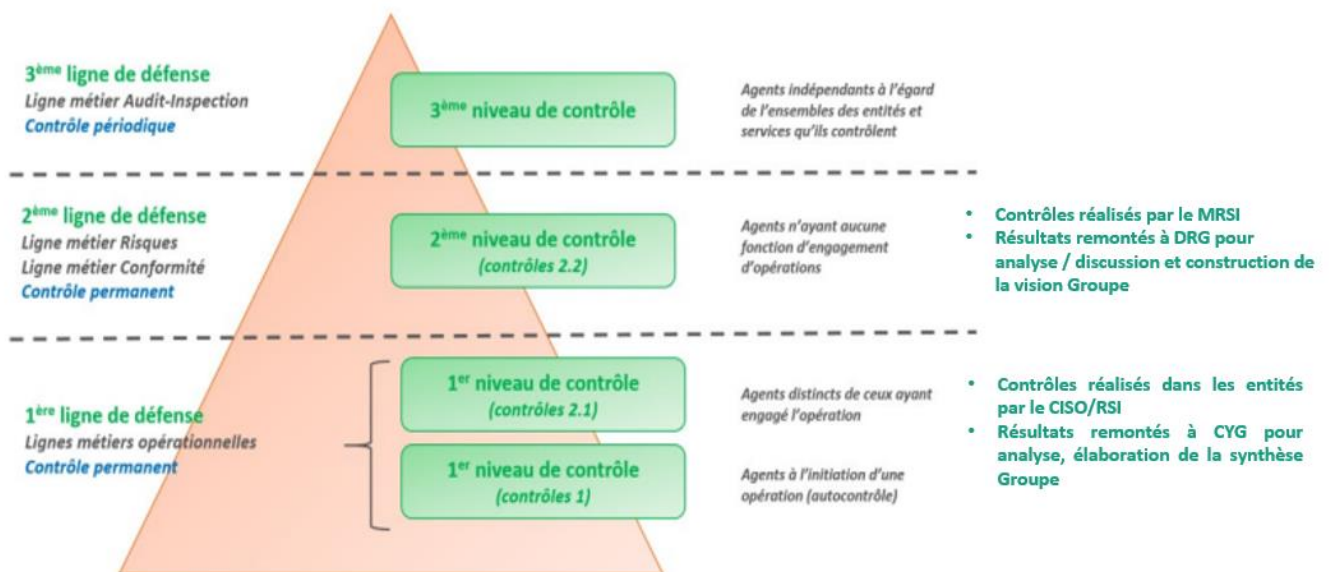


J'ai passé les quatre jours suivant dans cette équipe.

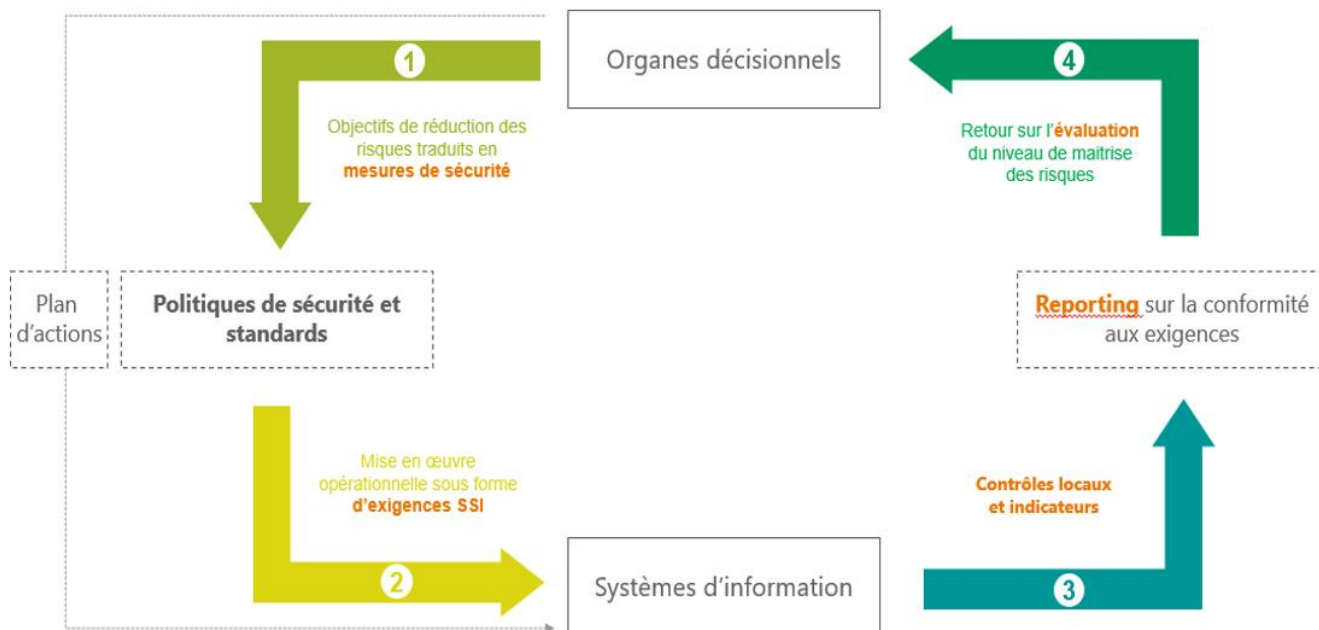
#### Plan de contrôle LOD1 (Evaluation et reporting)

Mission :

- Contrôler le 1<sup>er</sup> Niveau de contrôle de défense




- Réaliser des contrôles sur les politiques de sécurité et standards puis reporter sur la conformité aux exigences



## Thématiques du plan de Contrôle Lod1 cyber 2024

<b>Sensibilisation</b> 1 <ul style="list-style-type: none"> <li>Sensibilisation des utilisateurs du SI</li> </ul>	<b>Accès</b> 5 <ul style="list-style-type: none"> <li>Cycle de vie / Processus</li> <li>Habilitations</li> <li>Comptes et identités</li> <li>Contrôle des authentifications</li> <li>Traçabilité et détection</li> </ul>	<b>Architecture du SI</b> 9 <ul style="list-style-type: none"> <li>Sécurité des serveurs et des infrastructures</li> <li>Segmentation du SI</li> <li>Sécurisation de l'Active Directory</li> <li>Sécurité des postes de travail</li> <li>Sécurité des terminaux mobiles</li> <li>Sécurité apportée par les infrastructures d'hébergement et de raccordement à internet</li> </ul>	<b>Données</b> 5 <ul style="list-style-type: none"> <li>Obligations générales</li> <li>Protection des données dans l'environnement utilisateur</li> <li>Protection des données dans les systèmes et flux</li> </ul>	<b>Externalisées</b> 3 <ul style="list-style-type: none"> <li>Maîtrise de la pré-contractualisation</li> <li>Maîtrise de la contractualisation</li> <li>Maîtrise de la post-contractualisation</li> </ul>
<b>Evolutions</b> 3 <ul style="list-style-type: none"> <li>Méthodologie et formation</li> <li>Sécurisation du développement des applications 2SR et SIIS</li> <li>Recettes de sécurité</li> </ul>	<b>Obso et vulnérabilité</b> 2 <ul style="list-style-type: none"> <li>Identification et classification des actifs informatiques</li> <li>Gestion des vulnérabilités</li> </ul>	<b>Surveillance</b> 3 <ul style="list-style-type: none"> <li>Journalisation et détection</li> <li>Reuves, évaluations et tests de sécurité</li> <li>Détection des usages interdits</li> </ul>	<b>Crises cyber</b> 3 <ul style="list-style-type: none"> <li>Processus opérationnel</li> <li>Exercice de gestion de crise cyber</li> <li>Recensement des incidents et exploitation des retours d'expériences</li> <li>Incidents de sécurité</li> </ul>	<b>PSI</b> 4 <ul style="list-style-type: none"> <li>Plan de Continuité des Activités</li> <li>Redémarrage après incident physique (IPSI)</li> <li>Redémarrage après incident logique (ILSI)</li> <li>Reconstruction des postes de travail (IMPT)</li> </ul>



## Sauvegarde

2

Principalement orientée sur la réalisation d'un exercice de sauvegarde et l'existence d'outil de pilotage des sauvegardes.

- Reconstruction de l'AD
- Maîtrise des sauvegardes



## Sécurité du Cloud

3

Contrôles construits en collaboration avec les responsables de la définition du cadre normatif groupe. Cible spécifiquement les applications installées sur un cloud public et prend en compte le niveau de service (SaaS, IaaS et PaaS).

- Inventaire des solutions Cloud
- Passage au Centre de Référence Cloud (CRC)
- Mécanismes d'authentification



## Sécurité du SIA

3

Contrôles construits à partir du standard IN-G-28. Couvre en particulier la ségrégation des environnements, la gestion des accès et traces.

- Conformité des postes de travail selon le standard IN-G-28
- Maîtrise des accès aux environnements 2SR et gestion des accès au SIA
- Traçabilité des actions sur le SIA



## Cadre de maitrise des risques

2

Contrôles visant à s'assurer de la correcte déclinaison locale des exigences du cadre de maitrise des risques notamment en cas de non-conformité aux PSSI.

- Déploiement local du cadre de maitrise des risques
- Remontée des dérogations de niveau groupe

## Liste des contrôles du plan de Contrôle Lod1 cyber 2024

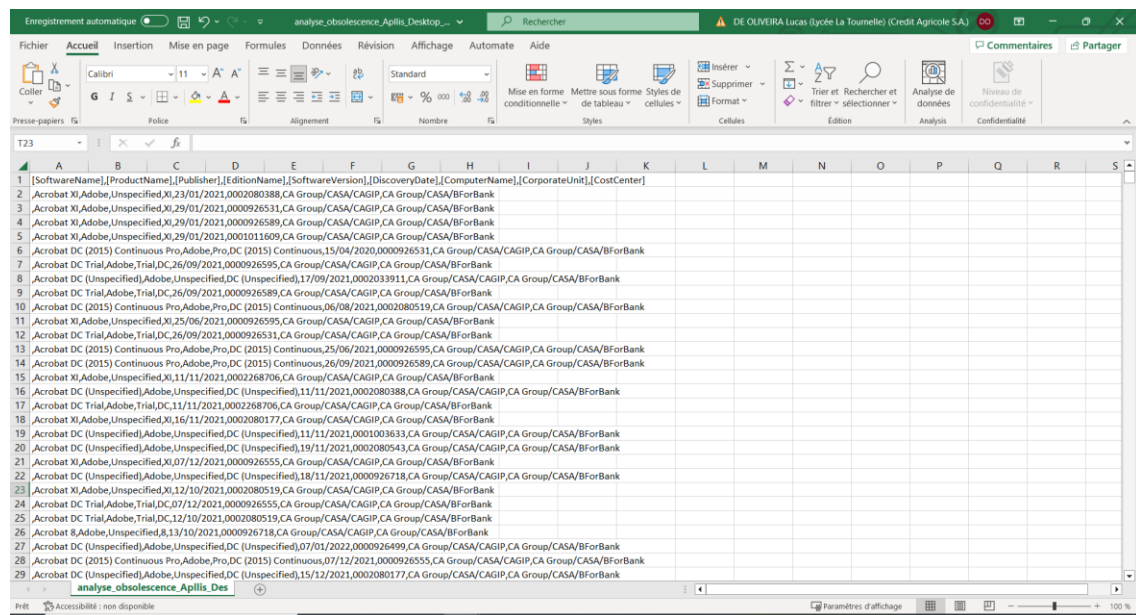
#	Thématique	#	Titre contrôle
1	Sensibilisation	1.1	Sensibilisation des utilisateurs du SI
2	Accès	2.1	Cycle de vie / Processus
		2.2	Habilitations
		2.3	Comptes et identités (personnes physique)
		2.4	Contrôle des authentifications
		2.5	Traçabilité et détection
3	Architecture	3.1	Sécurité des senseurs et infrastructures
		3.2	Segmentation du SI
		3.3	Sécurisation de l'Active Directory
		3.4	Sécurité des postes de travail : configuration, EDR et antivirus.
		3.5	Sécurité des postes de travail : administration, chiffrement, connexion des périphériques amovibles et applications autorisées.
		3.6	Protection du poste de travail et des terminaux mobiles vis-à-vis d'Internet par les infrastructures
		3.7	Sécurité des Terminaux mobiles : tablettes et smartphones
		3.8	Sécurité apportée par les infrastructures d'hébergement et de raccordement à Internet : tests d'intrusion et scans de vulnérabilité
		3.9	Sécurité apportée par les infrastructures d'hébergement et de raccordement à Internet : chiffrement et déclaration au CERT
4	Données	4.1	Obligations générales sur la protection des données
		4.2	Protection des données dans l'environnement utilisateur : supports amovibles
		4.3	Protection des données dans l'environnement utilisateur : postes de travail et partages réseaux
		4.4	Protection des données dans les systèmes et flux : chiffrement
		4.5	Protection des données dans les systèmes et flux : suppression / anonymisation des données
5	Externalisation	5.1	Maîtrise de l'externalisation : pré-contractualisation
		5.2	Maîtrise de l'externalisation : contractualisation
		5.3	Maîtrise de l'externalisation : post-contractualisation
6	Evolution	6.1	Méthodologie et formation
		6.2	Sécurisation du développement des applications 2SR et SIIS
		6.3	Recettes de sécurité
7	Maintenance	7.1	Identification et classification des actifs informatiques
		7.2	Gestion des vulnérabilités
8	Surveillance	8.1	Journalisation et détection
		8.2	Revue, évaluations et tests de sécurité
		8.3	Détection des usages interdits
9	Incidents cyber	9.1	Formalisation et tests du processus opérationnel de gestion des incidents cyber
		9.2	Reconement et exploitation des incidents cyber pour améliorer le dispositif de gestion de crise
		9.3	Incidents de sécurité
10	Plan de Secours Informatique	10.1	Plan de Continuité des Activités
		10.2	Redémarrage après incident physique (IPSI)
		10.3	Redémarrage après incident logique (ILSI)
		10.4	Reconstruction des PdT (IMPT) - (IMPT)
11	Sauvegarde	11.1	Reconstruction de l'AD
		11.2	Tests de restaurations
12	Sécurité du Cloud	12.1	Inventaire des solutions cloud
		12.2	Passage au CRC
		12.3	Cloud Mécanisme d'authentification
13	Système d'Information Administration	13.1	Conformité des postes de travail selon le standard IN-G-28
		13.2	Maîtrise des accès aux environnements 2SR
14	Cadre de maitrise des risques	14.1	Déploiement local du cadre de maitrise des risques
		14.2	Remontée des dérogations de niveau groupe

## Tâche réalisée :

J'ai pu faire une analyse d'obsolescence d'actifs logiciels sur excel :

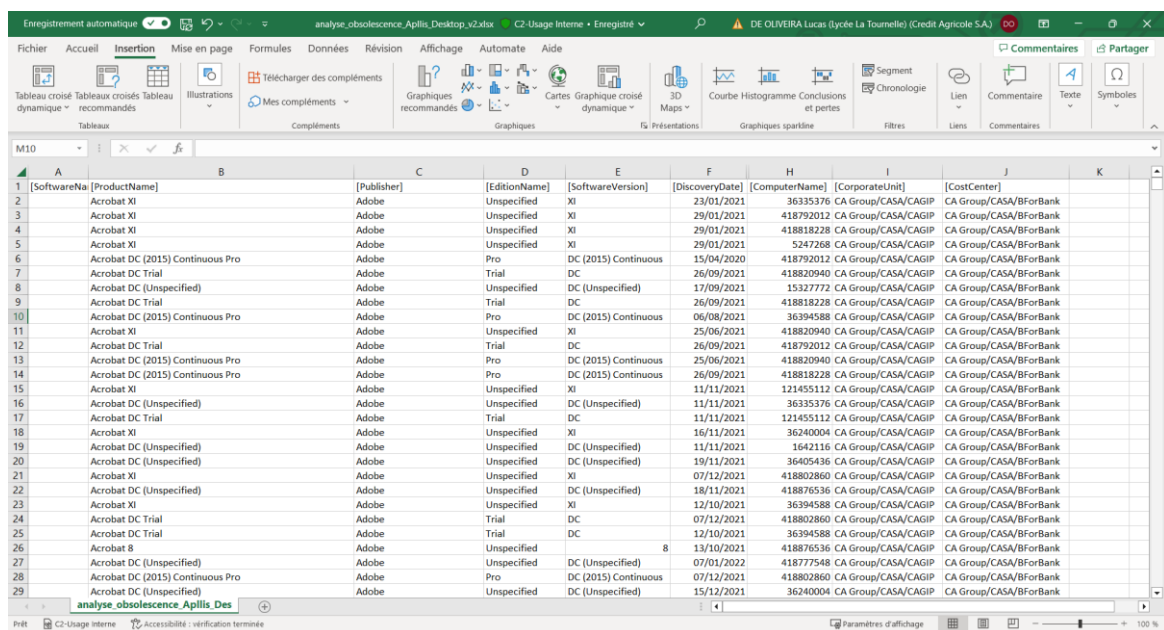
- Rendre lisible la page
- Trier les éléments

Avant



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	[SoftwareName]	[ProductName]	[Publisher]	[EditionName]	[SoftwareVersion]	[DiscoveryDate]	[ComputerName]	[CorporateUnit]	[CostCenter]										
2	Acrobat XI	Adobe,Unspecified,XI	23/01/2021	0002080388	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
3	Acrobat XI	Adobe,Unspecified,XI	29/01/2021	0000926531	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
4	Acrobat XI	Adobe,Unspecified,XI	29/01/2021	0000926589	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
5	Acrobat XI	Adobe,Unspecified,XI	29/01/2021	0001011609	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
6	Acrobat DC (2015) Continuous Pro	Adobe,Pro,DC (2015) Continuous	15/04/2020	0000926531	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
7	Acrobat DC Trial	Adobe,Trial,DC	26/09/2021	0000926595	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
8	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	17/09/2021	0002033911	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
9	Acrobat DC Trial	Adobe,Trial,DC	26/09/2021	0000926589	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
10	Acrobat DC (2015) Continuous Pro	Adobe,Pro,DC (2015) Continuous	06/08/2021	0002080519	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
11	Acrobat XI	Adobe,Unspecified,XI	25/06/2021	0000926595	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
12	Acrobat DC Trial	Adobe,Trial,DC	26/09/2021	0000926531	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
13	Acrobat DC (2015) Continuous Pro	Adobe,Pro,DC (2015) Continuous	25/06/2021	0000926595	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
14	Acrobat DC (2015) Continuous Pro	Adobe,Pro,DC (2015) Continuous	26/09/2021	0000926589	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
15	Acrobat XI	Adobe,Unspecified,XI	11/11/2021	0002268706	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
16	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	11/11/2021	0002080388	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
17	Acrobat DC Trial	Adobe,Trial,DC	11/11/2021	0002268706	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
18	Acrobat XI	Adobe,Unspecified,XI	16/11/2021	0002080177	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
19	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	11/11/2021	0001003633	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
20	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	19/11/2021	0002080543	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
21	Acrobat XI	Adobe,Unspecified,XI	07/12/2021	0000926555	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
22	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	18/11/2021	0000926718	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
23	Acrobat XI	Adobe,Unspecified,XI	12/10/2021	0002080519	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
24	Acrobat DC Trial	Adobe,Trial,DC	07/12/2021	0000926555	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
25	Acrobat DC Trial	Adobe,Trial,DC	12/10/2021	0002080519	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
26	Acrobat XI	Adobe,Unspecified,XI	13/10/2021	0000926718	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
27	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	07/01/2022	0000926499	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
28	Acrobat DC (2015) Continuous Pro	Adobe,Pro,DC (2015) Continuous	07/12/2021	0000926555	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													
29	Acrobat DC (Unspecified)	Adobe,Unspecified,DC (Unspecified)	15/12/2021	0002080177	CA Group/CASA/CAGIP	CA Group/CASA/BforBank													

Après



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1	[SoftwareName]	[ProductName]	[Publisher]	[EditionName]	[SoftwareVersion]	[DiscoveryDate]	[ComputerName]	[CorporateUnit]	[CostCenter]										
2	Acrobat XI	Adobe	Unspecified	XI		23/01/2021	36335376	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
3	Acrobat XI	Adobe	Unspecified	XI		29/01/2021	418792012	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
4	Acrobat XI	Adobe	Unspecified	XI		29/01/2021	418818228	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
5	Acrobat XI	Adobe	Unspecified	XI		29/01/2021	5247268	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
6	Acrobat DC (2015) Continuous Pro	Adobe	Pro	DC (2015) Continuous		15/04/2020	418792012	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
7	Acrobat DC Trial	Adobe	Trial	DC		26/09/2021	418820940	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
8	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		17/09/2021	15327772	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
9	Acrobat DC Trial	Adobe	Trial	DC		26/09/2021	418818228	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
10	Acrobat DC (2015) Continuous Pro	Adobe	Pro	DC (2015) Continuous		06/08/2021	36394588	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
11	Acrobat XI	Adobe	Unspecified	XI		25/06/2021	418820940	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
12	Acrobat DC Trial	Adobe	Trial	DC		26/09/2021	418792012	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
13	Acrobat DC (2015) Continuous Pro	Adobe	Pro	DC (2015) Continuous		25/06/2021	418820940	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
14	Acrobat DC (2015) Continuous Pro	Adobe	Pro	DC (2015) Continuous		26/09/2021	418818228	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
15	Acrobat XI	Adobe	Unspecified	XI		11/11/2021	121455112	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
16	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		11/11/2021	36335376	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
17	Acrobat DC Trial	Adobe	Trial	DC		11/11/2021	121455112	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
18	Acrobat XI	Adobe	Unspecified	XI		16/11/2021	36240004	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
19	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		11/11/2021	1642116	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
20	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		19/11/2021	36405436	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
21	Acrobat XI	Adobe	Unspecified	XI		07/12/2021	418802860	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
22	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		18/11/2021	418876536	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
23	Acrobat XI	Adobe	Unspecified	XI		12/10/2021	36394588	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
24	Acrobat DC Trial	Adobe	Trial	DC		07/12/2021	418802860	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
25	Acrobat DC Trial	Adobe	Trial	DC		12/10/2021	36394588	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
26	Acrobat XI	Adobe	Unspecified	XI		13/10/2021	418876536	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
27	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		07/01/2022	41877548	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
28	Acrobat DC (2015) Continuous Pro	Adobe	Pro	DC (2015) Continuous		07/12/2021	418802860	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										
29	Acrobat DC (Unspecified)	Adobe	Unspecified	DC (Unspecified)		15/12/2021	36240004	CA Group/CASA/CAGIP	CA Group/CASA/BforBank										

Ensuite j'ai transformé le tableau en un tableau croisé dynamique

Étiquettes de lignes	Nombre de Computer
Acrobat 6 Pro	12
5247268	1
6102452	1
36240004	1
36335376	1
36394588	1
116200160	1
121455112	1
418774384	1
418792012	1
418802860	1
418818228	1
418820940	1
Acrobat 7	24
1642116	1
5247268	1
6102452	1
33572300	1
36240004	1
36335376	1
36394588	1
36402724	1
36405436	1
116178464	1
116180724	1
116194284	1

Pour me permettre de faire une analyse d'élément de preuve pour vérifier si les logiciels sont obsolètes ou pas.

Pour en suite en déduire des plans d'actions.

## Les tableaux de bords

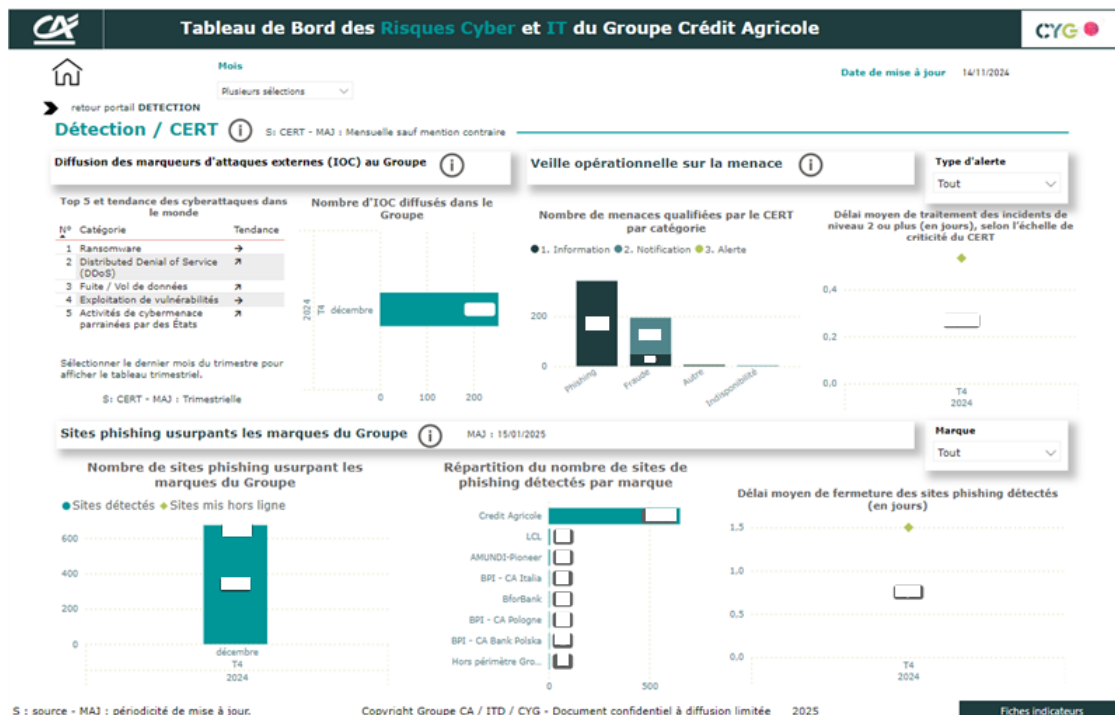
Pour les organisations, il est important de disposer d'un tableau de bord lié à la cybersécurité où dit de SSL, selon l'ANSSI, composé de nombreux indicateurs dont des indicateurs clés (KPI). Cela permet de centraliser les informations, de suivre les performances en matière de sécurité et de détecter rapidement les faiblesses et les anomalies.

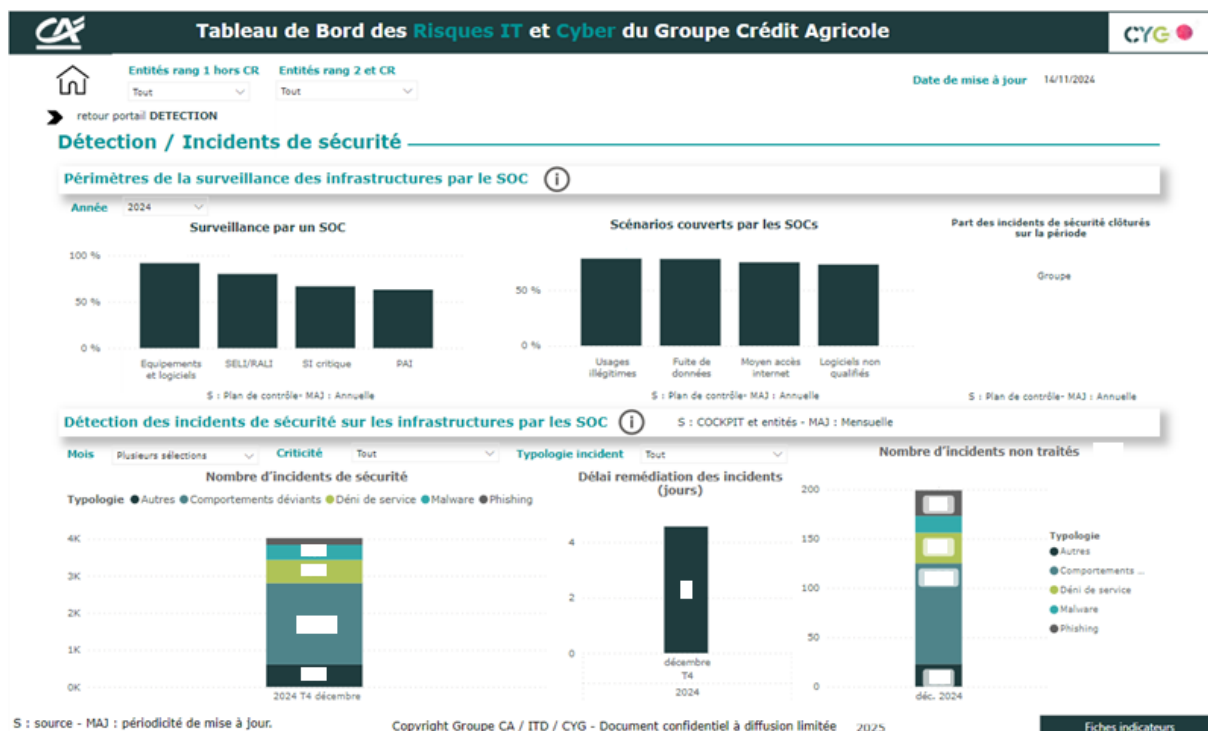
- Le Crédit Agricole a mis en place un tableau de bord des risques informatiques consultable à tout moment par les équipes CISO de chaque entité, ainsi que par la direction des risques du Groupe. Ce tableau de bord, conçu pour être un outil de référence fournit une vision globale et détaillée de la maturité du Groupe en matière de cybersécurité et de gestion des risques



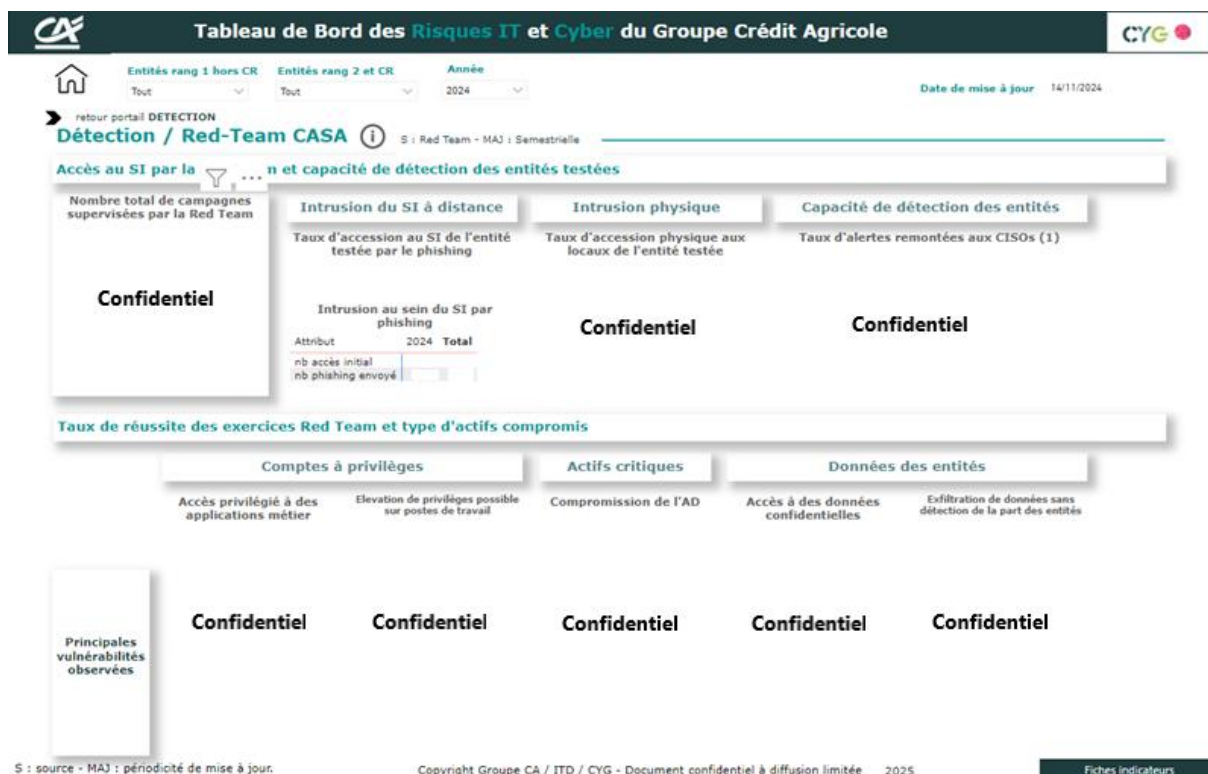
Hébergé sur la plateforme PowerBI, ce dernier permet aux équipes de visualiser et d'analyser les informations. Ils peuvent identifier rapidement les tendances, les anomalies, et obtenir des rapports détaillés qui facilitent la prise de décisions stratégiques. C'est tous les 6 mois (juillet/décembre) qu'ils le remplissent.

Voici un tableau de bord qu'il réalise :





## Bilan de la red team





Pendant une journée j'ai été avec Gilles Nerondat qui a travaillé au CERT et qui m'a expliqué les missions qu'il réalisait :

- Regarder les autres noms de domaine du Crédit Agricole pour contrôler les faux sites
- Gérer les attaques phishing
- Gestion de crise (réunion avec CISO + analyse forensic)

Il m'a également montré un rapport de pentest qui décrivait le contexte de la mission, les vulnérabilités trouvés et les solutions pour l'entreprise.

#### 4. CISO du Crédit Agricole SA



J'ai passé les trois jours suivant dans cette équipe.

**CISO (Chief Information Security Officer)** = responsable de l'évaluation des risques Sécurité de l'information et du pilotage des actions de réduction des risques correspondantes.

##### Missions

- **Sensibilisation**  
Exercices de faux phishing  
Outil utiliser bluesecure

**bluesecure**

- **Suivi des prestations externalisées**  
Contrats + CRC + DPIA  
OLVID
- **Contrôles et revues**  
LOD1 + 2.2C + Programme Habilitations  
Contrôles USB + Internet Etendu + ADML  
Revue Teams + Revue MyGuest + Revue Managériale
- **Comitologie**  
Réunion des différents comités du Crédit Agricole
- **Gestion des alertes, incidents et dérogations utilisateurs**  
Incidents SOC + alertes DLP

J'ai pu voir Tristan un consultant qui travaille sur des **CRC** (Centre de Référence Cloud), des revues d'habilitations, sur le comité de sécurité.

Leur équipe doivent aussi sensibiliser les RH sur le phishing car c'est les premières ciblent de ce type d'attaque.

## **CISO Adjoint (Denis Som mavilla)**

Vis ma vie CISO

### **Missions :**

- Réadapter les politiques chaque année
- Analyse du risque MESARI
- Validation de l'analyse de risque
- Assurer la sensibilisation sur le phishing (suivi des clics)
- Gérer les mails signaler
- Faire du whitelist (donner les droits aux URL pour ceux qui veulent y accéder)

Ils gèrent également des alertes **DLP**.

#### Outil :

**SAPIENS** est un site où le CERT publie les vulnérabilités + les descriptions de chaque menace

**Bluesecure** = outil qui crée des scénarios de phishing avec de l'IA

**DLP** = vérifier que les clients ne s'envoient pas des documents C3 ou C4

#### Henry

Il s'occupe des mails envoyés du SOC à propos des personnes du Crédit Agricole qui envoient des documents à une personne externe ou à eux même, il vérifie si les documents sont confidentiels. Pour cela il doit :

- Vérifier par exemple sur quel site la personne a partagé des documents, voir si le site web est suspect ou pas
- Vérifier l'adresse mail de la personne adressé si c'est une personne interne ou sur une adresse personnelle
- Demande à la personne dans un mail si c'est bien elle l'auteur de l'envoi des documents et une justification de cette envoie

#### **Campagne phishing**

Il fait 1 campagne de phishing tous les mois à tout le groupe CASA.

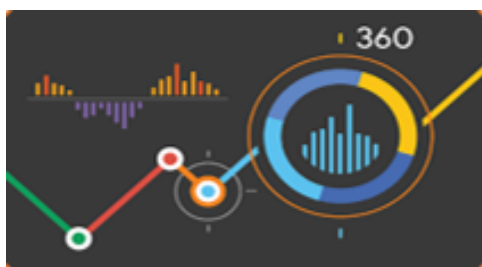
En envoyant un mail avec généralement un cadeau à la clé (mail de Noël) ou des problèmes d'identifiants (tentative de connexion)

#### Outil :

**Lucy Security** un logiciel pour l'hameçonnage mais ils vont changer d'outil pour **Bluesecure**.

**Jira** pour remonter les tickets

## 5. Risques IT



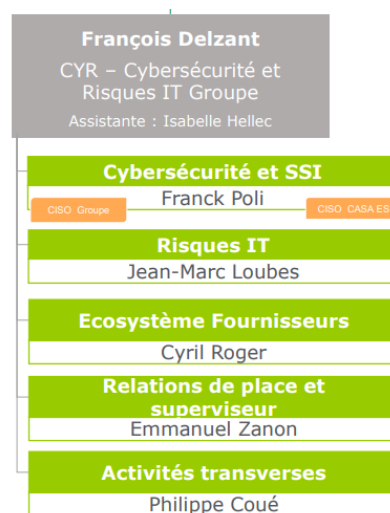
Ensuite j'ai passé une semaine dans cette équipe.

### Equipe Jean-Marc Loubes

J'ai été accompagné

William

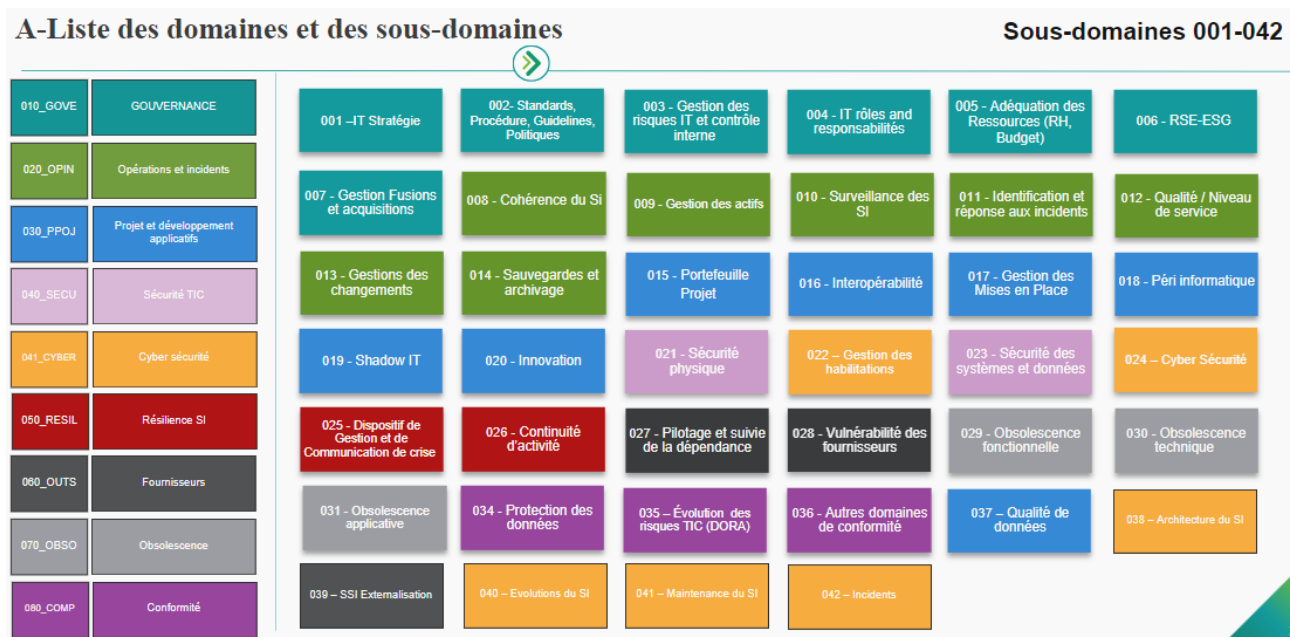
- Proposer une Nomenclature Groupe (actualisée / partageable) et accompagner au besoin les entités dans la déclinaison sur les 1ères lignes de défense (DSI)
- Mettre en commun nos éléments de langage et nos bonnes pratiques
- Disposer d'une vision globale et simple des risques
- Intégrer les travaux du Radar IT
- Renforcer la culture des risques TIC dans le groupe



Il définit les domaines puis les sous domaines

➔ Définition des risques

Projet GRC (Gestion Relation Client)



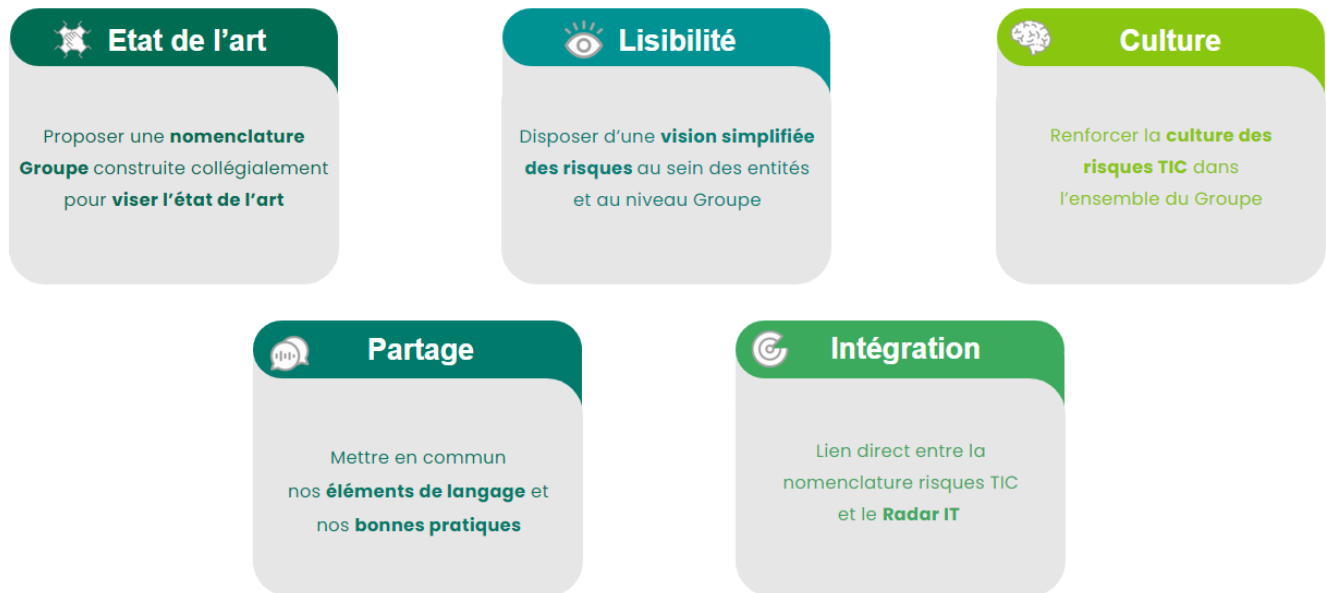
**Interopérabilité** : permet aux systèmes d'information de communiquer et de fonctionner ensemble sans restriction ni conflits. Une bonne interopérabilité assure que les différentes applications et infrastructures peuvent échanger des données et des services de manière fluide, ce qui améliore l'efficacité opérationnelle et réduit les coûts liés aux solutions de contournement.







**Shadow IT** : concerne l'utilisation de systèmes, de logiciels et de services informatiques sans l'approbation explicite du département IT. Le Shadow IT peut poser des risques importants pour la sécurité, la conformité et la gestion des ressources de l'entreprise.

Les risques TIC (Les Technologies de l'Information et de la Communication)

**1ère étape :** création d'une **nomenclature** des risques TIC partageable par l'ensemble des entités du Groupe

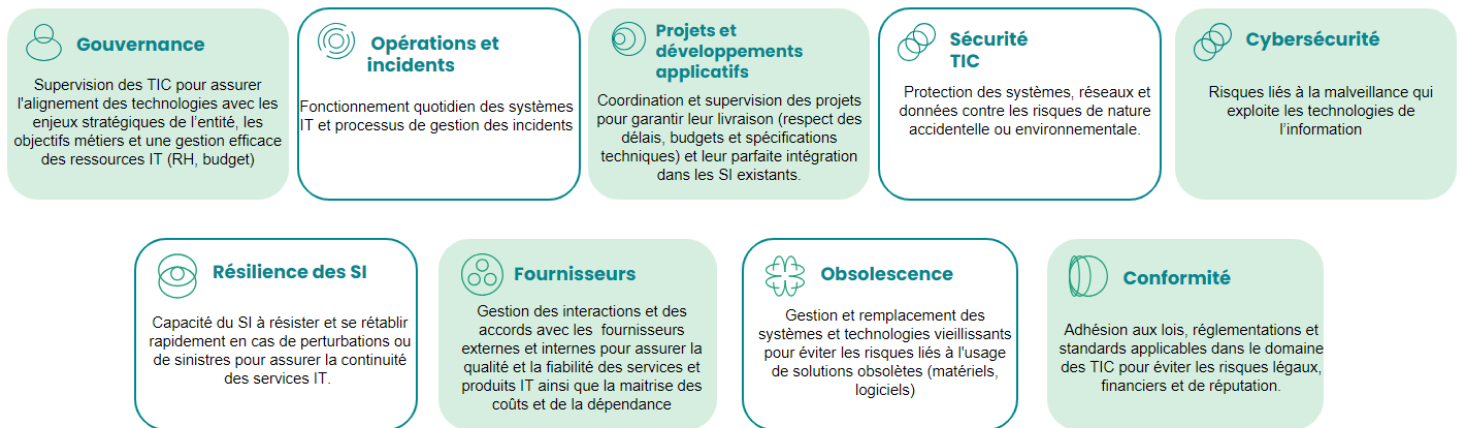
Une nomenclature définie pour répondre aux besoins de chaque entité



 Contraintes géographiques	 Contraintes sectorielles	 Contraintes réglementaires
<p>Des <b>règles pays</b> pouvant impacter l'organisation de la gestion des risques TIC</p> <p>.....</p> <p> Suisse : LPD OPD, LIMF</p> <p> USA : GLBA, FISMA</p> <p>• ...</p>	<p>Des entités attachant une priorité différente aux risques TIC</p> <p>.....</p> <p>en fonction de leur secteur d'activité, nécessitant de prendre en compte ces spécificités.</p> <p><i>Exemples : services de paiement, activités immobilières, secteur d'investissement</i></p>	<p>Différentes réglementations en vigueur ou en cours de validation impactant les attendus sur la gestion des risques TIC</p> <p>.....</p> <p></p> <ul style="list-style-type: none"><li>• <b>GDPR</b> (General Data Protection Regulation)</li><li>• <b>DORA</b> (Digital Operational Resilience Act)</li><li>• <b>AI Act</b> (Artificial Intelligence Act)</li><li>• <b>DSA</b> (Digital Services Act) / <b>DMA</b> (Digital Markets Act)</li><li>• <b>Cyber Resilience Act</b></li><li>• <b>Data Act</b></li><li>• <b>NIS Directive</b></li><li>• <b>IDAS Regulation</b> (Electronic Identification, Authentication and Trust Services)</li><li>• <b>Autres règlements</b> (Cybersecurity Act, ePrivacy Regulation, DSP3...) :</li></ul>

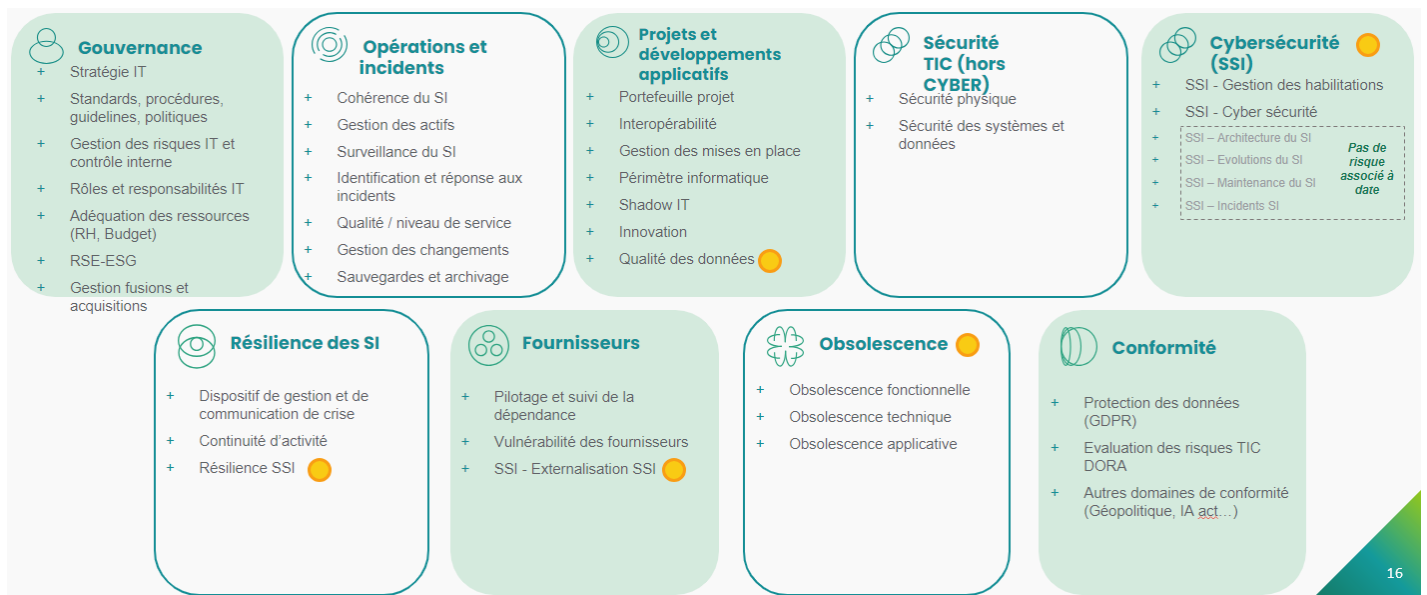
## Nomenclature risques TIC : 9 domaines de risque

définis sur la base des travaux réalisés au sein des entités, des évolutions réglementaires, des orientations de place et des évolutions technologiques/digitales



## Nomenclature risques TIC : 41 sous domaines de risque

garantissant la précision et l'exhaustivité de la nomenclature



### Outil utilisé :

#### Themerit

**KPI** (Key Performance Indicator) = indicateur utilisé pour l'aide à la décision dans les organisations.

**KRI** (Key Risk Indicators) = mesure utilisée en gestion pour indiquer le degré de risque d'une activité.

J'ai assisté à quatre visio sur plusieurs solutions de mesure de risque :

- IBM OnePages
- OneTrust
- Archer

Pour être plus précis dans les contrôles.

### Risque Transverse (ou risque de contagion de groupe) :

Il s'agit d'un risque qui, s'il se matérialise, **affecte simultanément ou en cascade un nombre significatif d'entités du groupe, voire l'ensemble du groupe.**

Le caractère transverse de ces risques signifie qu'ils ne sont pas confinés à une seule entité mais peuvent se propager et avoir des répercussions sur l'ensemble du groupe Crédit Agricole, affectant ainsi la continuité des opérations, la sécurité des données et la conformité réglementaire ou même l'image du groupe.

Un même risque selon les entités peut être considéré comme transverse alors même qu'il ne le serait pas pour une autre entité.

La gestion de ces risques mérite d'être traitée selon une approche organisationnelle globale groupe CA.

Ils sont soumis à la réglementation européenne **DORA**.



Le **Digital Operational Resilience Act (DORA)** est un règlement (n°2022/2554) adopté par l'Union européenne en décembre 2022 pour encadrer la cybersécurité des entités financières, telles que les banques et les établissements de crédit.

L'objectif final est de **maintenir la continuité opérationnelle** des services financiers au sein de l'Union européenne, même en cas de perturbations, d'incidents ou d'attaques. DORA marque **un changement de paradigme, le passage d'une vision défensive de la sécurité à une résilience globale** du secteur financier. Il ne s'agit plus seulement de se défendre, mais bien de résister.

## 6. Activités Transverses



J'ai passé une journée avec l'équipe

### Missions :

- Programmer des projets qui traitent un sujet de sécurité du groupe
- Sensibiliser avec des formations

# Conclusion

Ce stage au sein du pôle Cybersécurité Groupe (CYG) du Crédit Agricole m'a offert une immersion précieuse dans l'univers complexe de la cybersécurité au sein d'une entreprise d'importance vitale pour la France. J'ai pu toucher du doigt la diversité des enjeux, des processus et des stratégies nécessaires pour maintenir une posture de sécurité solide face à des cybermenaces en constante évolution.

Les missions qui m'ont été confiées m'ont permis d'acquérir des compétences techniques, telles que la gestion des vulnérabilités et l'analyse de données à l'aide d'outils comme PowerBI et Excel. J'ai également pu développer une vision globale de la gouvernance cyber et du rôle fondamental que jouent chaque équipe dans la sécurisation des systèmes d'information.

Ce stage m'a également permis d'évoluer dans un environnement où la collaboration et la coordination entre les différentes entités sont essentielles à l'efficacité des mesures de sécurité.

En conclusion, ce stage a confirmé mon intérêt pour le domaine de la cybersécurité et en particulier dans le pentesting. La rigueur, l'adaptabilité et la capacité à collaborer avec des équipes pluridisciplinaires sont des qualités que je retiendrai de cette expérience et qui me serviront dans la poursuite de ma carrière.