h e g

Haute école de gestion
Genève

Contrôles de sécurité contre la fuite et le vol de données dans un environnement bancaire

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Christian Luther DJOUMESSI TONFACK

Conseiller au travail de Bachelor :

Ciarán BRYCE, Professeur HES

Genève, le 26 juin 2020

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de gestion

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre Bachelor of Science HES-SO en Informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son conseiller au travail de Bachelor pour analyse par le logiciel de détection de plagiat URKUND, selon la procédure détaillée à l'URL suivante : https://www.urkund.com .

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 26 juin 2020

Christian Djoumessi

Remerciements

Je remercie mon directeur de mémoire, Monsieur Ciarán Bryce pour son aide et sa présence tout au long de la réalisation de ce travail. Ses conseils et son professionnalisme m'ont permis d'améliorer mon travail.

Je remercie ensuite mes maîtres de stage messieurs Philippe Emery et Eldo Mabiala, pour leur aide précieuse dans l'élaboration des thématiques abordées dans ce mémoire, ainsi que leurs conseils et idées hors du commun. Je leur suis reconnaissant pour le temps qu'ils m'ont accordé, la confiance qu'ils ont placée en moi et leur accompagnement dans le monde professionnel, plus précisément dans le secteur bancaire.

Je remercie également le groupe bancaire qui m'a employé, de m'avoir permis de réaliser ce travail en entreprise, et de rencontrer des personnes qui m'ont donné de précieux conseils, tant pour la réalisation de ce mémoire que dans ma vie professionnelle future.

Je remercie les membres de ma famille, mes proches et mes amis pour le soutien indéfectible et inconditionnel qu'ils m'ont apportés tout au long de cette formation, spécialement Audrey Tonfack et Eric Ladem pour avoir lu mon mémoire et apporté leur feedback.

Pour finir, je dédie ce travail à ma mère, qui serait très heureuse de voir le résultat de mon travail.

Résumé

Si on appelle le pétrole or noir, de nos jours, on pourrait appeler les données « or virtuel ». L'évolution constante des technologies de l'information engendre une augmentation exponentielle des données produites, notamment due à la nécessité des échanges d'information. Les données sont notamment importantes dans le monde des affaires car elles permettent de produire des informations qui, avec les outils de « Business Intelligence », aident à prendre des décisions. Dans certains secteurs d'activités, les entreprises collectent les données avec le consentement de leur propriétaires (pour les revendre et leurs modèles d'affaires sont basés là-dessus, ou pour améliorer l'activité en elle-même). Elles doivent donc être garantes des données collectées et doivent en assumer la protection face aux organisations ou personnes malveillantes qui collectent les données illégalement pour diverses raisons telles que la revente illégale, le chantage ou d'autres raisons malsaines.

Le secteur financier regorge de données qui peuvent avoir une valeur concurrentielle ou financière énorme. C'est pourquoi ce domaine d'activité est d'autant plus exposé à d'éventuelles menaces de vol, perte et de fuite de données.

En Suisse, la FINMA (l'autorité fédérale de surveillance des marchés financiers) émet des recommandations contraignantes afin de garantir la stabilité du système financier. Ces recommandations incluent les aspects de protection des données (Circulaire 2008/21 annexe 3). Il est primordial pour les institutions financières en Suisse de se mettre en conformité avec la FINMA, car le non-respect des recommandations en vigueur peut aller jusqu'au retrait de la licence permettant d'exercer.

Le groupe bancaire dans lequel j'ai réalisé ce travail (le Groupe, dans le reste du document) a mis en place sa politique interne de sécurité des systèmes d'information. Cette politique inclut la gestion des cyber-risques, parmi lesquels la fuite de données sensibles est un risque d'une haute importance. Divers moyens de protection face à ce risque sont mis en place tels que le chiffrement des données, le blocage des supports externes, le contrôle des périphériques, le contrôle du trafic, la revalidation des accès, etc). Dans le cadre de ce travail, nous évoquerons le contrôle du trafic, la revalidation des accès et d'autres éléments du système d'information ; gestion des événements de sécurité (SIEM), réponses aux incidents de sécurité et l'analyse des risques dans le cadre du déploiement d'une nouvelle technologie.

Table des matières

Contrôles de sécurité contre la fuite et le vol de données dans un environnement bancaire **1**

Déclaration ..... **i**

Remerciements ..... **ii**

Résumé ..... **iii**

Liste des tableaux ..... **vi**

Liste des figures ..... **vi**

1. Introduction **1**

2. Présentation du Groupe **3**

3. Fuite de données dans un environnement bancaire **5**

3.1 Définition de la fuite de données *5*

3.2 Causes de la fuite de données *5*

3.2.1 Convictions des lanceurs d'alertes 7

3.2.2 Raisons financières 7

3.2.3 Espionnage industriel 8

3.2.4 Sabotage 8

3.3 Canaux de fuite de données *9*

3.3.1 Papier 9

3.3.2 Électronique 9

3.3.3 Voix 9

3.4 Vecteurs de fuite de données *10*

3.4.1 L'être humain 10

3.4.2 Infrastructure et application informatique 10

3.5 Impact de la fuite de données pour l'entreprise *11*

3.6 Moyens de protection *12*

3.6.1 Sécurité du système d'information 12

3.6.2 Principe du « need to know » 13

3.6.3 Exercice de gestion de crise 13

3.6.4 Formation 14

4. Objectifs 15

5. Déroulement 16

5.1 Analyse de l'existant 16

5.1.1 Analyse de l'état des lieux actuel du DLP 16

5.1.2 Analyse de l'outil de traitement des logs 20

5.2 Gestion des risques internes 22

5.2.1 Configuration de l'outil DLP du Groupe 22

5.2.2 Participation à l'amélioration de règles de détection des fuites de données 31

5.2.3 Contribution à la gestion des incidents 35

5.3 Gestion des risques externes 38

5.3.1 Étude des éventuels contrôles DLP dans un environnement cloud 38

5.3.2 Initiation au SIEM 41

5.4 Revalidation des accès 42

5.4.1 Configuration de l'outil de supervision pour la revalidation des accès 43

5.4.2 Campagne de revue des accès aux applications critiques 43

5.4.3 Campagne de revue des accès aux répertoires sensibles 44

6. Analyse des objectifs 52

6.1 Objectifs du Groupe 52

6.2 Objectifs personnels 52

8. Conclusion 54

Bibliographie 56

Annexe 1 : Moyens de contrôles des risques liés au cloud 58

Annexe 2 : Échelles d'évaluation des risques du Groupe 59

Annexe 3 : RACI ISIR ..... Erreur ! Signet non défini.

Annexe 4 : Abréviations 61

Liste des tableaux

Tableau 1: Matrice des rôles et fonctionnalités DLP....23

Tableau 2: Tests DLP effectués....35

Tableau 3: Analyse des risques cloud....39

Tableau 4: Matrice d'évaluation des risques....59

Tableau 5: Codes couleurs des niveaux de risques....59

Tableau 6: Liste des abréviations....61

Liste des figures

Figure 1: Utilisation des données clients d'une banque....6

Figure 2: Réseau avec firewall....17

Figure 3: Magic Quadrant for Enterprise DLP....18

Figure 4: Magic Quadrant for SIEM....20

Figure 5: Corrélation des logs....21

Figure 6: Architecture DLP....25

Figure 7: Tableau de bord DLP....27

Figure 8: Planification automatique de la prise d'empreinte....28

Figure 9 : Condition de la règle Discovery....28

Figure 10: Plan d'action règle Discovery....28

Figure 11 : Paramétrage de l'OCR....29

Figure 12 : Processus de gestion des anomalies....30

Figure 13: Plan d'action règle DLP....34

Figure 14: Condition de la règle d'exception....34

Figure 15: Source de l'exception....34

Figure 16: Plan d'action de la règle d'exception 35
Figure 17: Rapport des tests DLP 35
Figure 18: Processus de réponse aux incidents 37
Figure 19 : Tableau de bord DLP - Trends 42
Figure 20: Varonis DataPrivilege 43
Figure 21: Revalidation des accès aux répertoires sensibles 45
Figure 22: Processus d'attribution des accès actuel 46
Figure 23: Processus d'attribution des accès amélioré 46
Figure 24: Synthèse des demandes 47
Figure 25: Droits d'accès et permissions 48
Figure 26: Création d'une permission 48
Figure 27: Sélection des utilisateurs liés à la création de la permission 49
Figure 28: Confirmation de la création de la permission 49
Figure 29: Droits d'accès et permissions de l'utilisateur ajouté 50
Figure 30: Révocation des droits d'accès 50
Figure 31: Droits d'accès et permissions - utilisateur révoqué 51
Figure 32: Moyen de contrôle des risques liés au cloud 58
Figure 33: Matrice RACI ISIR 60

1. Introduction

Le secteur financier, de par ses activités, est une mine de données sensibles. De ce fait, les entreprises de ce secteur sont des cibles importantes des personnes malveillantes qui ont pour objectif d'extorquer des données. Qu'elle soit intentionnelle ou non-intentionnelle, les conséquences de la fuite de données peuvent être énormes pour toutes entreprises.

Afin de protéger efficacement son système d'information et par conséquent ses données, une organisation financière doit se conformer aux attentes du régulateur. De ce fait, le Groupe, acteur reconnu dans le milieu bancaire en Suisse, doit donc mettre en place des contrôles et assurer l'efficacité de ces derniers, afin de réduire le risque de fuite de données. Dans ce cadre, ce travail a donc permis :

- D'accompagner l'équipe en charge de la cyber-sécurité en les aidant à préciser et documenter des procédures usuelles de contrôle
- De procéder à des tests et expérimentations pour améliorer le dispositif de contrôle en cyber-sécurité en particulier dans le domaine très règlementé de la protection des données
- De participer à l'encadrement d'un futur ingénieur dans le domaine de l'informatique par le biais du partage d'expérience pratique avec deux experts de la sécurité des systèmes d'information dans le milieu bancaire

Dans les sections à venir, nous évoquerons les points suivants :

- La présentation du Groupe
- La fuite de données dans un environnement bancaire
    - La définition de la fuite de données
    - Les causes de la fuite de données
    - Les canaux de fuite de données
    - Les vecteurs de fuite de données
    - L'impact de la fuite de données pour l'entreprise
    - Les moyens de protection
- L'objectif de ce travail
- L'analyse de moyens existants déjà dans le cadre de la lutte contre la fuite de données, et les améliorations apportées dans le cadre de ce travail. Nous parlerons des outils suivants :
    - L'outil DLP (Data Loss/Leakage Prevention) : Pour contrôler, détecter et empêcher la fuite de données
    - L'outil de traitement de logs : Pour collecter, centraliser et corréler les événements de sécurité
    - L'outil de revalidation des accès : Pour s'assurer que les accès ne sont attribués qu'aux ayant droits
- La mise en place du plan de réponse aux incidents de sécurité

- L’analyse des risques liés au cloud et la présentation d’une technologie DLP cloud
- La campagne de revalidation des accès

2. Présentation du Groupe

Fondé en 1996 à Genève, le groupe bancaire suisse en forte croissance, est axé exclusivement sur la gestion d'actifs via quatre métiers complémentaires :

- La banque privée de haut niveau
- La gestion d'actifs institutionnels
- Les gérants indépendants
- Les marchés privés

Le Groupe propose aux investisseurs un style d'investissement basé sur la gestion active et une gestion des risques visant une performance absolue. Le groupe dispose de fonds propres importants et jouit de son statut d'entreprise indépendante du fait de sa structure d'actionnariat familial.

Le Groupe met un accent particulier en ce qui concerne le traitement des données de ses clients, et fait donc face à des multiples défis, tant au niveau réglementaire qu'au niveau sécurité. Aux vues de ces derniers, le groupe se doit de se mettre en conformité avec les régulateurs des différents pays dans lesquels il exerce ses activités. En Suisse nous notons par exemple la FINMA, l'organisme qui définit les règles à tenir par les entreprises financières, telle que la directive 2008/21[1] qui table sur le risque opérationnel des banques. L'un des gros challenges des banques au niveau sécurité, est d'assurer la confidentialité des données clients. L'annexe 3 de la directive 2008/21 de la FINMA détaille entièrement ce point qui concerne précisément le traitement des données électroniques de clients. Cette annexe recense les éléments suivants, que doivent traiter les banques et notons que la liste est non-exhaustive :

- La définition des CID (Client Identifying Data) et la catégorisation des données clients
- Les règles et processus garantissant la confidentialité des données
- La classification des données clients confidentiels et la définition des niveaux de confidentialité
- La définition des responsables des CID
- La localisation du stockage des données (également à l'étranger)
- Principe du moindre privilège (Need to know)
- Le système d'autorisation des accès selon les rôles et responsabilités
- L'établissement des normes de sécurité en rapport avec la taille de la banque et le niveau de complexité de son système d'information informatisé
- Le processus d'identification des incidents liés à la confidentialité et le plan de traitement

[1] https://www.finma.ch/fr/~/media/finma/importiertedokumente/regulierung/anhoerungen/06-rundschreiben-operationelle-risiken/eb-rs-08-21.pdf?la=fr

- La mise en place de contrôles pour assurer l'amélioration continue des processus permettant de garantir la confidentialité des CID

Suite à l'entrée en vigueur de la RGPD (Règlement Général sur la Protection des Données) depuis le 25 mai 2018, une révision de la LPD (Loi sur la Protection des Données) a été lancée. Cette révision qui a commencé en 2017, est prévue d'entrer en vigueur en 2021 et intégrera la plupart des exigences de la RGPD. D'ici là, le groupe devra être en mesure de fournir à ses clients toutes les données de ces derniers qu'il traite et a en sa possession, à la demande. Dans un environnement où les données des clients sont traitées par plusieurs départements (par exemple au niveau du gestionnaire de clients, les risques, le juridique et conformité, le fichier central, la sécurité et le département informatique), il devient difficile de centraliser toutes les données d'un client. L'un des problèmes majeurs est aussi lié aux tendances des clients dans l'ère du numérique. Il existe un grand fossé à rattraper entre le secteur de la finance qui est très formel, et l'évolution du numérique qui amène des alternatives de communications informels mais rapide. On peut citer comme exemple un client qui communique ses ordres à son gestionnaire via l'application de messagerie WhatsApp, au lieu de passer par des procédures formelles avec des documents à traiter et signer, qui prennent souvent beaucoup de temps, et qui peuvent être fastidieux. Ceci ajoute donc une complication quant à la centralisation des données traitées.

3. Fuite de données dans un environnement bancaire

3.1 Définition de la fuite de données

Tous les jours, des millions de transactions bancaires sont effectuées. Ces transactions font donc de l'environnement bancaire un milieu riche en données telles que des CID[2], les relevés des comptes bancaires, les informations relatives aux actions, les obligations et les titres. Dans les systèmes d'information des institutions bancaires se trouvent également des informations stratégiques sur le fonctionnement de la structure, elles ne sont pas à négliger. Ces données, généralement à caractères sensible et confidentiel positionnent les banques très haut dans la liste des organismes ciblés par des hackeurs.

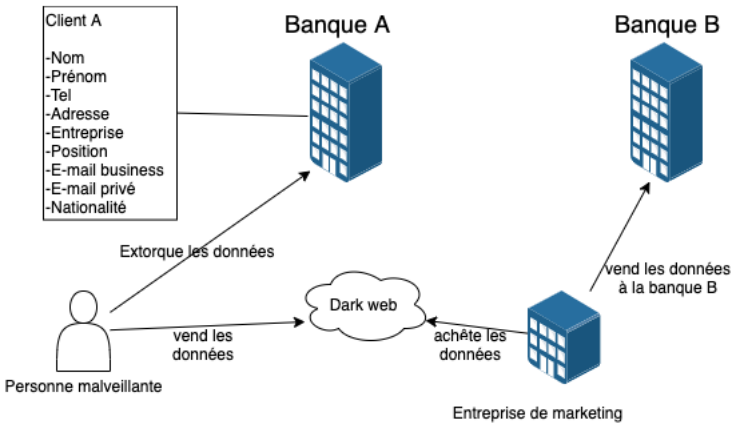
La fuite de données est le résultat d'un accès indu ou d'un transfert de données non-autorisé. Ceci mène à la violation de la confidentialité des données, qui est un principe de base en matière de sécurité de l'information.

3.2 Causes de la fuite de données

Les données font partie des éléments stratégiques et fondamentaux pour l'aide à la prise de décision. De la même manière que les données des personnes donnent des informations irréfutables sur les personnes physiques et morales ; les données d'entreprises parfois révèlent l'identité de l'entreprise ainsi que d'autres informations spécifiques à celle-ci. Les données que détient une entreprise ou les données qu'elle produit, pourraient représenter un avantage concurrentiel. La figure ci-dessous montre l'exemple des parties intéressées par un document bancaire ; le formulaire A. Ce formulaire est rempli par les clients lors de l'ouverture d'un compte dans une banque.

[2] La définition d'un CID est propre à chaque entreprise. Pour le Groupe, il s'agit d'une donnée qui mène à l'identification d'un client, directement ou indirectement. Par exemple le nom, prénom, numéro de compte bancaire, numéro de passeport, etc.

Figure 1: Utilisation des données clients d'une banque



(Christian Djoumessi)

Dans ce cas de figure, plusieurs scénarios sont possibles :

- La personne malveillante qui extorque les données clients pour :
  - Vendre dans le « dark web[3] »
  - Usurper l'identité du client à des fins malsaines
  - Faire du chantage à la banque A, car l'identité des clients est une donnée protégée par le secret bancaire en Suisse
- L'entreprise de marketing pourrait acheter les données clients dans le « dark web » pour :
  - Proposer des produits et services aux clients
  - Vendre les données à une tierce partie (banque B)
- La banque B quant à elle pourrait acheter ce type de données afin d'atteindre les personnes fortunées et proposer leur services (par exemple un placement avec un taux de rendement supérieur à celui de la banque A)

Ces scénarios montrent que les données peuvent avoir une valeur financière, dans la mesure où celui qui les possède peut en tirer un profit en numéraire. Pour une entreprise, prendre conscience de la valeur de ses données permet de définir le niveau de protection adéquat de celles-ci et de planifier les investissements en matière de cyber sécurité. Les données d'une entreprise sont hétérogènes et toutes ne nécessitent pas une protection renforcée. Par exemple investir dans des solutions de sécurité pour sécuriser les photos non-confidentielles ou les e-mails non liés aux affaires de l'entreprise parait, selon des cas de figure, insensé. Par contre, dans le domaine bancaire, il est nécessaire voire impératif d'investir dans la sécurité des données stratégiques et des données clients parce qu'elles ont une valeur économique (puis que monnayable) et que leur

[3] Le « dark web » aussi appelé le « dark net » est un réseau parallèle à internet, se reposant sur ce dernier, et n'est qu'accessible via des logiciels spécifiques.

protection est réglementée par le régulateur. Et leur perte peut causer des dommages coûteux, difficilement réparables et surtout porter atteinte à l'image de l'entreprise.

Les motivations de la fuite de données sont très diverses. Dans un environnement bancaire, les données peuvent fuiter à l'intérieur (par des personnes faisant partie de l'environnement) ou l'extérieur (très souvent des hackeurs).

3.2.1 Convictions des lanceurs d'alertes

Les convictions des lanceurs d'alertes sont également des éléments déclencheurs de fuite de données. Dans cette catégorie, il existe plusieurs cas tels que :

Hervé Falciani

Ancien informaticien de la filiale suisse de la banque HSBC, il est aujourd'hui reconnu comme l'un des lanceurs d'alerte les plus célèbres. Il est connu pour avoir fait fuiter les informations impliquant plus de 130 000 comptes bancaires provenant de la banque HSBC, lorsqu'il travaillait chez ce dernier. En 2006 lorsqu'il réorganisait la base de données au sein de HSBC, il avait constaté que cette base de données favorisait l'évasion fiscale. Le nouveau système qu'il a proposé n'a pas été retenue, ce qui l'a motivé à commettre ce délit.

Rudolf Elmer

Condamné par la justice suisse en 2011 pour violation du secret bancaire, il avait divulgué via Wikileaks des informations concernant les activités de la banque Julius Bär sur l'évasion fiscale. Sa motivation était de dénoncer les manipulations illégales de son institution. Il était commissaire aux comptes de la banque Julius Bär entre 1994 et 2002.

Christoph Meili

Il est le premier citoyen helvète à avoir obtenu l'asile politique aux USA. Ancien agent de sécurité à l'UBS (Union Bank of Switzerland) à Zurich, il est connu pour avoir fait fuiter des documents bancaires découverts dans la salle de destruction de documents de l'UBS. Ces documents, datant de 1945 à 1965 prouvaient l'existence des fonds et titres de patrimoines fonciers juifs saisis par le régime nazi, dissimulés en Suisse. Il a dérobé des documents physiques, ensuite il a livré ces documents à une organisation juive.

3.2.2 Raisons financières

Les raisons financières sont aussi à l'origine des fuites de données. Il est commun pour des personnes malveillantes, très souvent des hackers, d'exfiltrer des données afin de les revendre, très souvent dans le « dark web ». Notons par exemple en cette période critique ou le monde est sévit par la pandémie du Covid-19 et le mot d'ordre est le confinement. Plusieurs travailleurs sont

amenés à faire du télétravail. Les visioconférences sont multipliées et l'application Zoom, qui offre ce service de visioconférence a vu son utilisation augmenter jusqu'à en devenir l'un des outils incontournables du télétravail. Victime de son succès, en quelques semaines, Zoom a été au centre d'un scandale dans lequel plus de 530 000 comptes utilisateurs dérobés de l'application ont été trouvés en vente sur le « dark web ». Les données trouvées contenaient des e-mails et mot de passe des utilisateurs, et des URL (Uniform Resource Locator) de réunions privées. Certains de ces comptes trouvés étaient même offerts gratuitement afin de favoriser le « zoom bombing », une pratique qui consiste à s'introduire dans une visioconférence privée sans en avoir l'autorisation.

3.2.3 Espionnage industriel

L'espionnage industriel, est également un facteur non-négligeable. Dans la guerre de rivalité entre entreprises, parfois, tous les risques sont pris pour arriver à ses fins. Par exemple en décembre 1965, quelques années avant le premier vol du Concorde, Sergueï Pavlov alors directeur de l'entreprise Aeroflot à Paris, est arrêté par la police française. Suite à une fouille de ses bagages, les enquêteurs ont récupéré des informations confidentielles tels que des plans détaillés des freins et du train d'atterrissage de l'avion franco-britannique. En fin décembre 1968, les russes ont fait décoller le prototype de l'avion de ligne nommé Tupolev Tu-144. Réplique du supersonique européen, cet avion était en partie le résultat de l'espionnage industriel des industries françaises de Sud-Aviation (Aérospatiale) coordonné par la direction générale des renseignements de l'État-Major des armées russes.

3.2.4 Sabotage

Il arrive parfois que faire fuiter les données d'une personne ou une organisation est utilisé comme moyen de pression au concerné dans le but soit de porter atteinte à son image, soit de demander une rançon. L'affaire Clearstream et la campagne présidentielle d'Emmanuel Macron illustre bien ce phénomène.

Affaire Clearstream

En mai 2004, le magistrat français Renaud Van Ruymbeke a reçu deux courriers anonymes, accompagnés de listing bancaires dénonçant des personnes ayant des comptes dissimules chez Clearstream, société financière luxembourgeoise. Dans le deuxième listing, se trouvait le nom de l'ex-président français, Nicolas Sarkozy. En mai 2006, Jean-Louis Gergorin, ami de Dominique de Villepin, alors premier ministre français au moment des faits, a reconnu avoir été l'auteur des listings avec la complicité de ce dernier. Le magistrat Renaud Van Ruymbeke a pu prouver que les documents bancaires reçus avaient été fabriqués, retirant ainsi les soupçons à l'endroit de Nicolas Sarkozy.

MacronLeaks

Proche de la fin de la campagne pour l'élection présidentielle 2017 en France, Wikileaks a révélé la fuite de grandes quantités de documents donnés à l'équipe de campagne d'Emmanuel Macron. Suite à cela, ces documents ont été lourdement retransmis sur les réseaux sociaux. Les documents contenaient des discussions privées du l'équipe du candidat à la présidence à cette époque, des photos, des notes confidentielles incluant des documents financiers. Les données piratées représentaient quasiment plusieurs gigaoctet, qui ont été dévoilées au grand jour à deux jours seulement du deuxième tour à l'élection présidentielle française. Une enquête a donc été ouverte au parquet de Paris, suite à la retransmission de ces documents sensibles sur internet.

3.3 Canaux de fuite de données

L'être humain étant le premier facteur de risque de fuite de données, il suffit d'une discussion orale pour faire fuiter des données. Cela dit, on ne peut pas complètement empêcher la fuite de données, on ne peut que réduire le risque qu'elle survienne.

Les canaux de fuite de données étant diverses, les plus récurrents seront présentés dans les paragraphes qui suivent.

3.3.1 Papier

Dû à l'évolution numérique, le taux de manipulation des données sur format papier a diminué, mais reste toujours considérable. Comme le souligne l'entreprise TAGIT EAS Technologies, malgré la croissance des outils de technologies IT (Information Technology), la fuite de données confidentielles causée par les documents papiers n'a pas été réduite. Il est très facile de faire fuiter les informations via ce canal, comme cela a été le cas pour Christoph Meili d'UBS, car très peu d'entreprises sont équipées d'un scanner pour analyser continuellement tout objet qui sort de l'entreprise (tel que les scanner dans les aéroports), ou alors d'un détecteur de papier.

3.3.2 Électronique

De nos jours, la voie électronique est le canal le plus utilisé pour manipuler les données, et donc les exfiltrer. Mais également, c'est le canal le plus facile à contrôler, via des outils de contrôle de sécurité tel que DLP que nous allons présenter dans ce travail, et d'autres outils de sécurité des systèmes d'informations.

3.3.3 Voix

Plus difficile à contrôler, ce moyen de fuite de données restera toujours d'actualité. Un des moyens utilisés pour exfiltrer des données en utilisant le canal vocal est l'hameçonnage par téléphone (Vishing). C'est une pratique d'ingénierie sociale qui consiste à passer par un appel téléphonique pour amener la cible à fournir des données personnelles ou confidentielles. Un scénario de vishing est le suivant :

- Une personne appelle le manager RH (Ressources Humaines) d'une banque et se fait passer pour un employé de la sécurité de cette banque
- La personne fait comprendre au RH qu'il y a eu une possible fuite de données provenant de son compte
- La personne demande ensuite au RH ses informations de connexion pour accéder aux différents comptes de la banque
- Se disant qu'il n'y a rien de suspect car la personne se présente comme un employé de la banque, et aussi aux vues du contexte de sécurité suscitant un sentiment d'urgence, le RH lui fournit les informations demandées

Les moyens de limiter la fuite de données via ce canal sont :

- L'application du principe du « need to know », que nous allons présenter dans ce document
- La sensibilisation des collaborateurs
- Le call-back qui consister à rappeler, quand cela est possible, la personne qui vous a appelé, sur un numéro connu qui est sensé être le sien

Le call-back a ses limites, car il ne fonctionne que si vous êtes appelé par une personne que vous êtes sensé connaître (un collègue, un client, un prestataire de service).

3.4 Vecteurs de fuite de données

3.4.1 L'être humain

L'être humain est le maillon faible en ce qui concerne la fuite de données. Le créateur de l'Observatoire du crime organisé à Genève avait signalé que la plupart des fraudes économiques au sein des organisations viennent de l'interne. Ceci est due au fait que les employés connaissent les mesures de protection et peuvent donc chercher les moyens de contournement. Le côté non-intentionnel est aussi à prendre en considération. Un employé peut maladroitement envoyer des données à l'extérieur en se trompant de destinataire. Chose courante, lors de l'écriture d'un e-mail, si l'auto-remplissage est actif sur le champ dédié à l'adresse e-mail du destinataire, il serait possible de se tromper d'adresse. Le Groupe a spécialement développé un module pour réduire ce risque.

3.4.2 Infrastructure et application informatique

L'utilisation des outils informatiques en entreprise et même à titre personnel est de plus en plus courant. Ces outils informatiques permettent d'accéder, traiter et transmettre des données plus rapidement et simplement. Bien qu'elles facilitent et améliorent le travail au quotidien, ces outils ne sont pas souvent sous le contrôle total de l'entreprise. Ceci engendre donc un risque quant au stockage et la manipulation des données.

Avec l'arrivé du cloud computing et tous ses bienfaits, les entreprises ont tendance à migrer une partie du stockage de leurs données et infrastructures en mode IaaS (Infrastructure as a Service)[4] vers le cloud. D'un point de vue utilisateur, cette solution peut être bénéfique car l'expertise du fournisseur cloud en matière de sécurité sera exploitée. Mais d'un autre point de vue, il y a une perte de contrôle sur l'ensemble des avoirs et des données de l'entreprise sur le cloud.

Les vulnérabilités rencontrées dans les solutions informatiques, peuvent permettre à une personne malveillante d'en abuser pour en extraire des données. Ces vulnérabilités incluent les équipements d'infrastructure périmétriques (premier point d'accès au réseau d'entreprise tels que les points d'accès Wi-Fi ou les commutateurs réseaux), les applications et terminaux mobiles ou fixes.

Concernant les applications, le réseau social à plus de 2 milliards d'utilisateurs, Facebook et l'entreprise britannique Cambridge Analytica ont été au centre d'une fuite massive de données impactant de dizaines de millions d'utilisateurs. Cambridge Analytica a récolté via Facebook les données des utilisateurs à leur insu pour ensuite les revendre à des entités politiques. Le parti républicain mené par Donald Trump, a notamment travaillé avec ce cabinet d'analyse durant la période des élections présidentielles des États Unis en 2016. Les données recueillis ont aidé l'équipe de Donald Trump à davantage viser les personnes susceptibles de le voter pendant la campagne présidentielle.

3.5 Impact de la fuite de données pour l'entreprise

Selon l'ampleur de la fuite de données et l'exploitation de celle-ci, les conséquences peuvent avoir de lourds impacts à l'endroit de l'entreprise affectée, telles que :

- Réputation et image
    - Les banques privées tiennent énormément à leur réputation et leur image car, ce sont des facteurs très souvent déterminants pour un client, une institution ou une haute personnalité (dans le cadre du marketing par exemple) dans le choix d'une banque avec qui collaborer
- Fiabilité
    - La perte de fiabilité implique également une perte de confiance tant au niveau des clients de la banque, qu'au niveau des employés. Un client qui n'a plus confiance à sa banque aura tendance de s'en lasser. Du côté de l'employé, son niveau d'implication dans ses tâches pourra certainement baisser
- Sanctions juridiques

[4] IaaS est un type de service cloud qui permet l'externalisation des serveurs de fichiers, serveurs de stockage et l'infrastructure réseau vers un fournisseur de service cloud, tel que Microsoft Azure.

    - En cas de fuite de données d'un client bancaire, celui-ci pourrait poursuivre sa banque en justice
    - Pour le non-respect de la protection de données, une entreprise peut se faire amender par une autorité juridique compétente. En Europe par exemple, des amendes sont prévus selon le cas de fuite de données en lien avec la RGPD
- Baisse du prix de l'action
    - Prix de l'action suit la loi de l'offre et la demande. En cas de fuite de données d'une entreprise côté en bourse, les détenteurs d'actions vont vouloir vendre leurs actions, mais la demande sera aussi impactée. Cette situation fera donc baisser le prix de l'action
- Perte de compétitivité
    - En lien avec la perte de clientèle, une entreprise se verra en perte de vitesse dans son domaine métier. Pour les banques privées qui en générale se mesurent en terme d'AuM (Asset under Management), la fermeture des comptes entraîne la réduction potentielle d'AuM
- Perte de clientèle
    - Les clients, surtout dans le secteur de la banque privée, tiennent à ce que leur banque ait une certaine stabilité, sans laquelle ils verront leurs avoirs dans la banque à risque
- Perte de secret industriel ou propriété intellectuelle
    - La fuite de données stratégiques pour l'entreprise, par exemple une banque, peut empiéter sur la confidentialité de leur savoir-faire dans le métier, qui pourra être exploité par des concurrents

Ces conséquences citées ont souvent un impact affectant les finances de l'entreprise touchée, ce qui peut donc mener à sa faillite.

Il est recommandé de gérer une telle crise de la façon la plus professionnelle et transparente possible en informant les autorités compétentes dans le domaine d'activité (c'est une obligation récente du 7 mai 2020 de la FINMA)[5] et les parties prenantes impactées (clients, fournisseurs, partenaires, etc.) et de se fier à ses processus préparés lors des exercices de gestion de crises.

3.6 Moyens de protection

Dans l'arsenal de solution pour se protéger contre le vol d'information, il y a avant tout la sécurité physique qui est essentielle mais que nous n'aborderons pas ici. Nous allons plutôt nous focaliser sur les processus et solutions informatiques.

3.6.1 Sécurité du système d'information

La sécurité du système d'information repose sur quatre principes : Confidentialité, intégrité, disponibilité et non-répudiation. Que ce soit au niveau individuel ou au sein d'une entreprise, la

[5]https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20200507-finma-aufsichtsmitteilung-05-2020.pdf?la=fr

bonne application de ces principes permet de garantir un certain niveau de sécurité et de se prémunir contre de potentielles vulnérabilités. La fuite de données relève de l'aspect confidentialité des données, et afin de renforcer cet aspect, il est important d'avoir au moins les outils suivants :

- Outil de corrélation de logs
    - Lors de l'analyse des incidents, il faut avoir les traces ou l'historique des événements pour aider à découvrir ce qui s'est passé, la cause de l'incident et comment y remédier
- Outil DLP
    - Outil pour contrôler, détecter et empêcher la fuite de données
- Gestion des identités
    - Identifier qui fait quoi, tous les profils doivent être personnels, aucun compte générique ne doit être toléré pour un employé
- Outil pour le contrôle des périphériques
    - L'exportations des données doit être contrôlée avec un outil centralisé

Dans le cadre de ce travail, nous allons aborder plus en détail les points DLP et outil de corrélation de logs.

3.6.2 Principe du « need to know »

En français "Principe du moindre privilège", selon lequel les acteurs d'un système d'information n'ont accès qu'aux informations dont ils ont besoin pour effectuer leurs tâches. Cet élément constitue une base solide en termes de sécurité des données, car il permet de renforcer la confidentialité des données. Si les données ne sont strictement accessibles qu'aux ayants droits, cela rendra la tâche difficile aux personnes malveillantes qui souhaitent y accéder. Dans ce cas de figure, les personnes les plus à risque de faire fuiter les données sont celles qui ont accès aux données, en conformité avec la politique de gouvernance des données de l'entreprise en vigueur.

3.6.3 Exercice de gestion de crise

Il est important de mettre en place un plan d'action de gestion de crise, en l'occurrence une crise liée à la fuite de données doit être anticipée. Ceci afin de réagir rapidement et d'apporter des solutions adaptées à la situation si une telle crise venait à se produire. Si une politique DLP est établie, elle doit contenir un processus d'identification de la gravité de la fuite et le processus d'escalation lié.

Outre le fait que le plan d'action doit être clairement documenté (Imposé par la FINMA et la RGPD), les scénarios contenus dans ce plan doivent être testés en conditions réelles afin d'être prêt à faire face à une telle situation.

3.6.4 Formation

La sécurité devrait être une affaire de tous. En entreprise, il est nécessaire que l'ensemble des employés aient un certain niveau d'éducation afin d'être en mesure d'aider l'entreprise dans l'amélioration continue de sa protection. Pour arriver à cela, il est important de garantir les points suivants :

- Sensibilisation des employés
- Formation des équipes IT et sécurité sur les nouvelles menaces et comment y faire face
- Formation éthique des employés
    - Ce point est souvent négligé, pourtant son importance est tout de même majeure, comme le souligne juge Treccani au sujet des informaticiens qui ont usuellement accès à plusieurs données sensibles : *« Il y a des lacunes énormes en ce qui concerne l'éthique des informaticiens, estime le juge vaudois. Dans leur formation, il n'y a aucun cours sur ce sujet. Lorsque je les interroge, je m'aperçois que la plupart considère qu'il est tout à fait normal qu'ils disposent de tous les accès. »*
    (largeur.com/ ?p=3078, lundi 15 février 2010)

4. Objectifs

Dans le cadre du cursus Bachelor of Science en informatique de gestion, il est obligatoire de réaliser un travail de diplôme.

Le Groupe travaille actuellement sur l'amélioration de ses procédures et processus en matière de gestion des risques internes et externes. En ce qui concerne les risques informatiques, les actions d'amélioration vont dans le sens de l'optimisation des contrôles.

L'objectif de ce travail est de participer à l'optimisation des contrôles liés à la gestion du risque de fuite et de vol de données sensibles. La fuite de donnée est supervisée au sein du Groupe par plusieurs fonctions notamment au travers des outils de prévention et détection, ainsi que par le contrôle des accès au système d'information. De ce fait, le périmètre défini pour atteindre cet objectif est le suivant :

Gestion des risques internes :

- Configuration de l'outil DLP du Groupe
- Participation à la gestion de règles de détection des fuites de données
- Contribution à la gestion des incidents

Gestion des risques externes :

- Étude des éventuels contrôles pour prévenir la fuite de données dans un environnement Cloud
- Mise en place d'au moins deux contrôles
- Initiation au SIEM (Security Information and Event Management) du Groupe

Revalidation des accès :

- Configuration de l'outil de supervision pour la revalidation des accès
- Campagne de revue des accès aux applications critiques
- Campagne de revue des accès aux répertoires sensibles

L'exécution de ces tâches permettra :

- A titre personnel, de découvrir les métiers de gestion des risques IT/les métiers de sécurité opérationnelle dans un environnement réel en production
- Pour le Groupe, accompagner les équipes dans la prévention du risque de fuite de données
- Au niveau académique, apporter un aspect pratique à mon cours de gouvernance de la sécurité suivi en deuxième année

5. Déroulement

5.1 Analyse de l'existant

En plus de l'assistance à l'équipe de sécurité des systèmes d'information, dans ses tâches quotidiennes, le présent travail portera sur l'utilisation des outils de gestion des risques suivants :

- Outil DLP
- Outil de traitement des logs
- Outil de revalidation et gestion des accès

Dans les paragraphes qui suivent vous trouverez un état des lieux des différents outils.

5.1.1 Analyse de l'état des lieux actuel du DLP

Définition

Le concept DLP est l'ensemble des stratégies, processus opérationnels et moyens techniques qui permettent de détecter, protéger et contrôler la fuite d'informations, en s'appuyant sur un référentiel de données. Les outils DLP sont des logiciels qui permettent d'analyser les informations transmises à des destinations non-autorisées (données en mouvement) et les informations stockées à des endroits également non-autorisés (données au repos). Le dispositif DPL n'est en général pas adapté pour les données en cours utilisation.

En ce qui concerne les données en mouvement, généralement, les entreprises utilisent les outils DLP pour analyser les informations qui sortent du réseau d'entreprise via les canaux e-mail, imprimante, web, disque externe et messagerie instantanée. Mais il est à noter que chaque entreprise adapte sa stratégie DLP en fonction des besoins métiers, et peut donc être amené à analyser également le trafic interne.

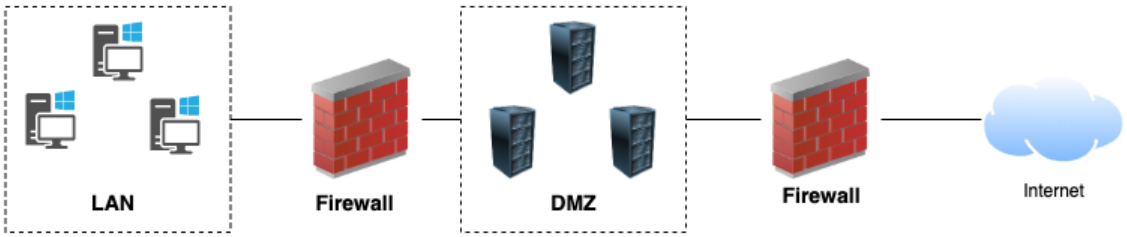
Différence entre le DLP et le pare-feu

On pourrait facilement confondre le DLP et le firewall(pare-feu). Ce dernier est un outil de sécurité qui permet de contrôler le type de communication entre deux réseaux. Un pare-feu en générale représente une barrière de sécurité entre un réseau interne et internet. Selon les règles définies dans le pare-feu, les paquets de communication transitant le pare-feu sont soit rejetés soit autorisés à traverser le réseau. Il existe plusieurs types de pare-feu tels que :

- Pare-feu par proxy
- Pare-feu sans état
- Pare-feu dynamique
- Pare-feu d'application web
- Pare-feu de nouvelle génération (Next Generation Firewall - NGFW)

Le Next Generation Firewall prend en compte les fonctionnalités des pare-feu traditionnels et y ajoute d'autre d'autres éléments de surveillance tels que l'IPS (Intrusion Prevention System), IDS (Intrusion Detection System), l'inspection du trafic TLS/SSL (Transport Layer Security/Secure Socket Layer), QoS (Quality of Service), etc pour appliquer son filtrage de communications, afin de ne pas se limiter aux informations contenues dans l'entête des paquets telles que l'adresse IP source et destination, l'interface réseau et le port UDP (User Datagram Protocol) ou TCP (Transport Control Protocol). Ceci repousse les limites des pare-feux traditionnels en filtrant les communications entrantes et sortants à plusieurs autres couches du modèle OSI, renforçant ainsi la sécurité. Comme information en plus, ce type de pare-feu intègre les données venant de sources tierces, par exemple l'annuaire LDAP (Lightweight Directory Access Protocol) pour identifier les utilisateurs dans les règles de filtrage.

Figure 2: Réseau avec firewall



(Christian Djoumessi)

A la différence du firewall qui analyse le contenu des paquets (et les utilisateurs pour le NGFW), la configuration des règles DLP prend en compte les éléments suivants :

- L'utilisateur source
- Les canaux de communications sortants (Web, SMTP, périphériques externes, messagerie instantanée et imprimantes)
- Les paramètres des données (données chiffrées, format de fichier, etc)
- Les expressions régulières (numéro de compte bancaire, numéro de carte de crédit, etc)
- Les empreintes de données (document interne, document sensible, base de données, etc)

On peut donc noter que les différences qui existent entre le DLP et le NGFW sont les suivants :

- La charge utile des données (le message réel, aussi appelé le « payload » en anglais) est analysée par DLP et non par le NGFW
- Aussi le DLP permet d'analyser les données au repos sur des terminaux, les données échangées en interne et les tentatives de communications, tandis que le NGFW analyse uniquement les données en mouvement d'un réseau vers un autre

Forcepoint DLP

Forcepoint DLP est l'outil DLP utilisé au sein du système d'information du Groupe. Cet outil est classé leader selon le rapport « Magic Quandrant for Enterprise DLP » de Gartner en février 2017.

Figure 3: Magic Quadrant for Enterprise DLP

(Gartner – Février 2017)

Éléments du DLP

Le DLP pièce angulaire pour protéger la fuite de données, est composé de plusieurs éléments qui vont être décrit ci-dessous :

Serveur de management DLP :

Ce composant est le cœur du système DLP. Tous les autres composants DLP s'enregistrent et se synchronisent avec le serveur de management. Ce dernier fait la corrélation des événements reçus pour afficher les informations telles que les anomalies DLP détectées et l'état des différents composants. C'est également dans ce composant qu'on configure les règles DLP. Ce serveur est aussi utilisé comme robot principal d'indexation pour les scans « discovery » que nous verrons plus bas dans ce document.

Serveur OCR (Optical Recognition Character) :

Comme le nom de ce composant l'indique, c'est le serveur qui permet d'analyser les fichiers de type image qui traversent les canaux réseaux, tels que les pièces jointes, les publications web et les impressions. Lorsque le trafic sortant comprend une image, ce serveur va vérifier si l'image est textuelle. Si oui, le texte compris dans l'image sera extrait et analysé afin de vérifier si le contenu est sensible. Ce composant peut également servir pour détecter les informations sensibles sur les fichiers se trouvant dans le réseau, lors d'un scan « discovery ».

Protector web :

Ce composant est utilisé pour intercepter le trafic web via le protocole ICAP (Internet Content Adaptation Protocol) et remonte les événements au serveur de management.

Protector mail :

Ce composant analyse le trafic SMTP (Simple Mail Transfer Protocol) et remonte les événements au serveur de management.

Analytics engine :

Ce composant est utilisé pour calculer le risque des événements de chaque utilisateur. Il est ensuite corrélé avec d'autres événements risqués pour enfin attribuer un score de risque par utilisateur. Les informations de ce composant sont remontées au serveur de management, qui affiche dans son tableau de bord le niveau de risque par utilisateur. Cette information est utile pour identifier les utilisateurs présentant un niveau de risque élevé afin de prendre des mesures de remédiation ou anticiper les futures actions.

Agents endpoint client :

Localement installé sur les terminaux (PC et serveur citrix), ce composant se synchronise avec le serveur de management pour recevoir les configurations DLP, et envoie à ce dernier les anomalies détectées.

Le trafic interne via l'application de collaboration interne est également filtré, et Il est à noter que le trafic entrant n'est pas filtré (volontairement).

Documentation des règles DLP

Un certain nombre de règles sont opérationnelles. Pour des raisons de confidentialité, ces règles ne seront pas détaillées. Une documentation des règles existe. En comparant cette documentation avec les règles actuellement utilisées, il en ressort que :

- 25% des règles actuellement utilisées sont documentées
- La documentation n'est pas à jour

Due au fait que les ressources humaines sont limitées et que la documentation est souvent une tâche moins prioritaire pour les ingénieurs, ceci a pour conséquences des lacunes pour démontrer la connaissance des règles en place dans les systèmes de protection lors d'audits ou de situations d'urgentes investigations. De ce fait, l'une des missions de ce travail de diplôme est d'avoir 100% des règles documentées et également mettre en place un processus de gestion de cette documentation.

5.1.2 Analyse de l'outil de traitement des logs

En informatique, les logs sont des enregistrements automatiques (historique) et horodatés concernant des événements d'un système ou d'un réseau. Il est a noter que les logs ne sont pas normés, donc diffèrent d'un système à l'autre.

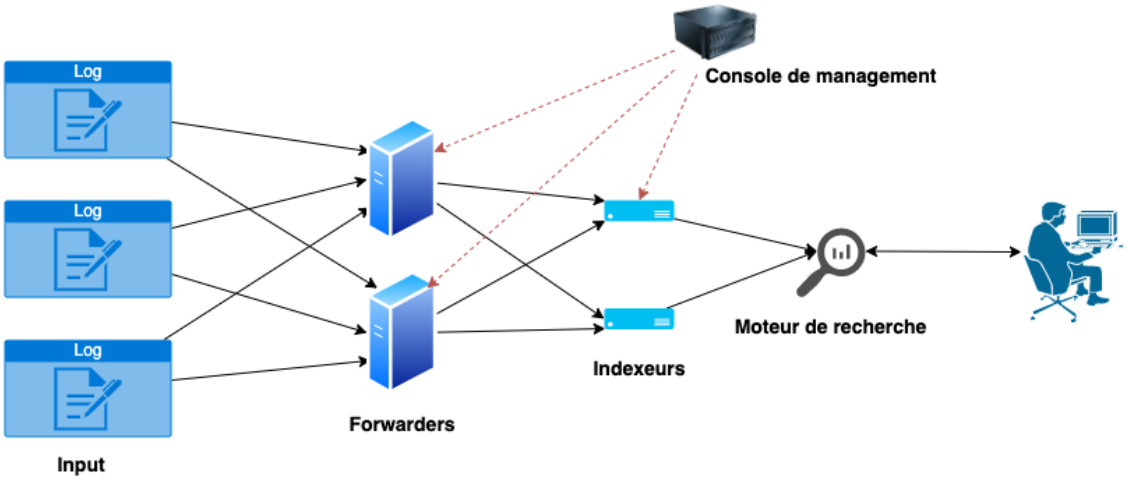
Le Groupe dans son système d'information utilise le SIEM Splunk Enterprise pour le traitement de log. Splunk est classé leader selon le rapport « The 2020 Magic Quadrant for SIEM ».

Figure 4: Magic Quadrant for SIEM

(Gartner – Février 2020)

Cet outil permet de collecter, indexer et corréler plusieurs logs provenant de divers éléments du système d'information, pour produire des informations lisibles et compréhensibles par tous en temps réel. Les informations produites peuvent être sous forme de graphique, tableau ou alerte.

Figure 5: Corrélation des logs



(Christian Djoumessi)

Les logs provenant de plusieurs sources sont collectés par l'outil de traitement des logs du système d'information du Groupe, que nous n'allons pas détailler. Dans le cadre de ce travail, nous allons nous limiter uniquement aux logs provenant de l'outil DLP.

Actuellement, il existe deux tableaux de bords qui permettent d'afficher les informations provenant des événements DLP, à savoir :

- DLP Tracking
- DLP Frequency

DLP Tracking

Ce tableau de bord permet d'afficher toutes les anomalies DLP déclenchées par l'envoie d'email, sous forme de tableau, avec les colonnes :

- Date et heure de l'anomalie
- Utilisateur source de l'anomalie
- Destinataire
- Sujet de l'email
- Nom de l'attachement
- Nombre d'occurrence d'éléments déclencheurs (matches)
- Nom de la police
- Destinataire client ou non

Ce tableau de bord permet de filtrer les anomalies du tableau selon les critères suivants :

- Intervalle de date et heure
- Nom de la police
- Afficher les anomalies avec comme destinataire un client

- Le nombre de matches au minimum
- L'utilisateur source de l'anomalie
- Le nom de domaine du destinataire
- L'adresse email du destinataire
- Le nom de l'attachement

DLP Frequency

Ce tableau de bord permet d'afficher sous forme graphique, la fréquence d'anomalies générées par utilisateur. On peut filtrer par l'intervalle de date et le nom de l'utilisateur. Les anomalies prises en compte concernent uniquement les emails qui ne sont pas destinés aux clients du Groupe.

5.2 Gestion des risques internes

Les risques internes, souvent apparentées aux risques opérationnels, sont des risques provoqués par des événements à l'intérieur d'une organisation. Il en existe plusieurs tels que les vulnérabilités des systèmes, la fraude interne, etc. Dans le cadre de ce travail nous traiterons uniquement le risque lié à la fuite de données. Dans le sous-chapitre qui suit, nous allons entrer dans l'aspect technique de l'outil DLP, qui nous permet de réduire ce risque.

5.2.1 Configuration de l'outil DLP du Groupe

Dans ce sous chapitre, nous allons entrer dans l'aspect technique de l'intégration de Forcepoint DLP dans le système d'information du Groupe. Pour cela, nous allons passer en revue les points suivants :

- Rôles et responsabilités des personnes ayant accès à la console de management DLP
- L'architecture DLP
- Quelques fonctionnalités clés
- Cas d'usage pratique

5.2.1.1 Rôles et responsabilités

Le DLP analyse toutes les actions vers les canaux cités dans les chapitres précédents. Ceci amène à une visualisation des informations très confidentielles dans la console de management DLP. C'est pourquoi il est nécessaire de définir des rôles et responsabilités des personnes y ayant accès, afin de ne pas porter atteinte à la confidentialité des informations qui s'y trouvent.

Nous allons commencer par définir les rôles et responsabilités, et ensuite présenter la matrice des fonctionnalités associées à chaque rôle. Les rôles suivants sont utilisés :

- Super Administrateur
    - Plus haut niveau de privilège
    - Mot de passe divisé en 2 parties et stocké dans un emplacement sécurisé. L'utilisation du compte associé à ce rôle doit être validé par :

        - Le CISO (Chief Information Security Officer)
        - Le CIO (Chief Information Officer)
        - Le COO (Chief Operating Officer)
- Auditor
    - Utilisé par le responsable du risque, l'audit et le control interne pour faire des audits périodiques des processus DLP
- External consultant
    - Utilisé pour corriger les aspects techniques de l'outil DLP
- System admin
    - Responsable de la maintenance technique de l'outil DLP
- Security
    - Premier niveau d'analyse des anomalies. Effectue le triage des événements et escalade les anomalies définies comme incidents au rôle Security escalation
- Escalation
    - Rôle assigné aux mêmbres du comité décisionnel pour confirmer la sévérité d'un incident de fuite de données. Le mot de passe du compté lie est changé après chaque utilisation
- Security escalation
    - Utilisé pour le deuxième niveau d'analyse d'événements (anomalies classées comme incident)

Le tableau suivant présente les rôles et responsabilités :

Tableau 1: Matrice des rôles et fonctionnalités DLP

Fonctionnalité	Super administrator	Auditors	External consultant	System admin	Security	Escalation	Security escalation
Statut global	X		X		X	X	X
Synthèse des rapports DLP	X	X	X		X	X	X
Afficher les éléments de violation	X				X	X	X
Afficher le classement des incidents par risque	X	X	X		X	X	X
Afficher la source et la destination des anomalies	X				X	X	X

Afficher les forensics[6]	X					X	X
Gestion des règles DLP	X				X	X	
Vue sur l'échantillon des empreintes de base de données	X					X	X
Afficher les logs de trafic	X		X	X	X	X	X
Afficher les logs du système	X		X	X	X	X	X
Afficher les logs d'audit	X	X	X	X	X	X	X
Paramètre généraux	X		X	X			
Déployer les modules systèmes	X		X	X			
Déployer les profils endpoint	X		X	X			
Déployer les paramètres	X		X	X	X	X	X

(Mon employeur)

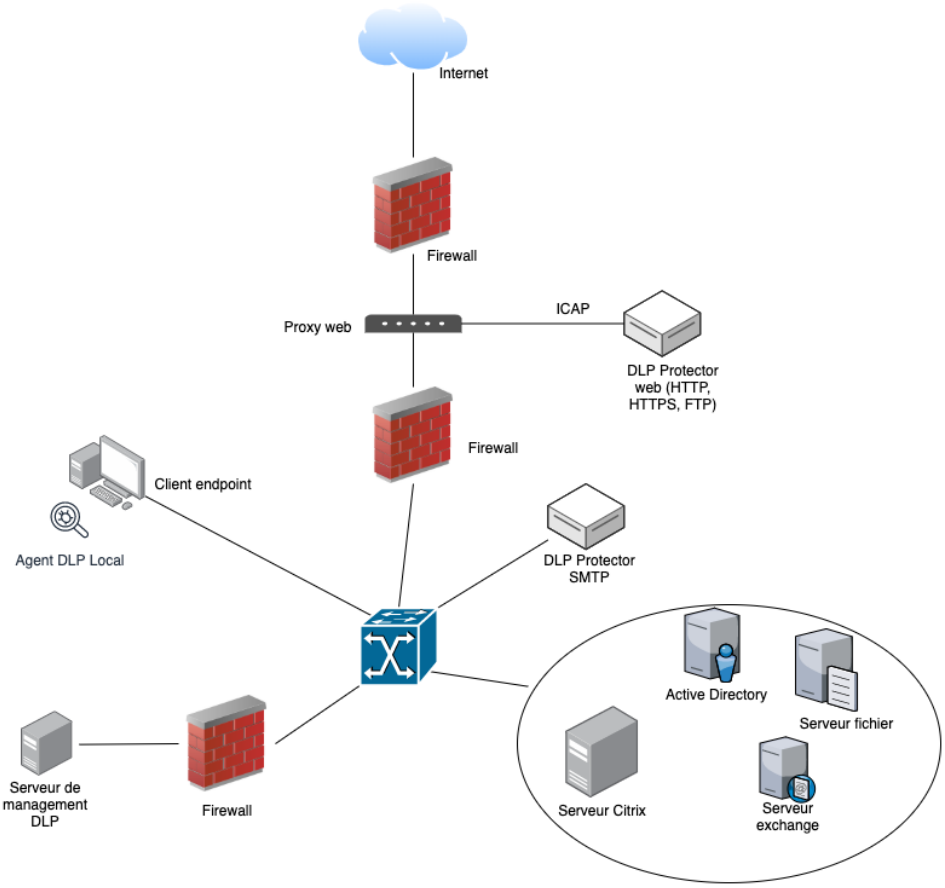
La fonctionnalité qui permet la gestion des règles DLP est l'une des plus importantes, donc il est important de limiter l'accès à cette fonctionnalité à des personnes clés (tels que le CISO ou le CSO). Le rôle « Security » est associé aux analystes de premier niveau. Afin d'avoir une meilleure ségrégation des responsabilités et de limiter le risque de fuite de données en interne, ce rôle (« Security ») ne devrait pas pouvoir faire des droits de lecture et écriture des règles DLP et en même temps avoir une vue sur les anomalies et logs générés.

5.2.1.2 Présentation de l'architecture

L'architecture nous permet de visualiser comment les composants DLP sont intégrés à l'architecture réseau au sein du groupe. Pour des raisons de confidentialité, cette architecture est simplifiée et montre uniquement les composants nécessaires à l'intégration du DLP. Donc ne reflète pas l'architecture dans son intégralité.

[6] En français « médecine légale »

Figure 6: Architecture DLP



(Mon employeur)

5.2.1.3 Quelques fonctionnalités clés (OCR – Discovery – Référentiel de recherche)

Référentiel de recherche

Lors d'une analyse, le DLP se sert d'un ou plusieurs référentiels comme base afin de faire la comparaison avec les données analysées. Les types de référentiels sont les suivants :

- Motif et phrase
- Propriétés de fichiers (fichier encrypté, format pdf, etc)
- Empreinte d'un fichier
- Empreinte d'une base de données

Pour le référentiel motif et phrase, on peut définir une expression régulière, une phrase clé ou un dictionnaire de phrases clés. La phrase clé et le dictionnaire de phrases clés sont faciles à définir, par contre l'expression régulière selon le cas, peut être subtile à définir.

Exemples d'expressions régulières

Exemple 1 : Adresse IP

L'expression régulière suivante correspond à n'importe quelle adresse IP :

\b(25[0-5]|2[0-4][0-5]|1[0-9][0-9]|1[0-9]|[1-9])\.

(25[0-5]|2[0-4][0-5]|1[0-9][0-9]|1[0-9]|[1-9])\.

(25[0-5]|2[0-4][0-5]|1[0-9][0-9]|1[0-9]|[1-9])\.

(25[0-5]|2[0-4][0-5]|1[0-9][0-9]|1[0-9]|[1-9])\b

Exemple 2 : Date

L'expression régulière suivante correspond à l'importe quelle date au format DD-MMM-YYYY :

\b\d{1,2}-[a-zA-Z]{3}-\d{3}\b

En définissant une expression régulière qui sera utilisée par les règles DLP, il est très important de la définir de manière à respecter précisément le domaine de définition du type de donnée, sinon définir le domaine qui se rapproche le plus possible au type de donnée. Si cela n'est pas respecté, le risque d'avoir de faux positifs devient élevé. Par exemple concernant l'expression régulière de l'adresse IP, on pourrait aussi la définir de la manière suivante « \b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\ », ce qui est plus simple que le premier exemple, mais le domaine de définition est plus large. Elle prend en compte le motif suivant « 999.999.999.999 » ce qui n'est pas une adresse IP.

Discovery

La fonctionnalité discovery de Forcepoint DLP permet d'analyser les données au repos sur les terminaux (PC, serveurs, etc) ou emplacements réseaux. Cette fonctionnalité peut être effectuée par trois composants :

- Le serveur de management et le serveur OCR pour effectuer le discovery sur les emplacements réseaux
- L'agent endpoint DLP pour effectuer le discovery sur les terminaux fixes

Une fois que les données analysées correspondent à une règle, le plan d'action associé à cette règle est lancé. Le plan d'action définit l'action à entreprendre une fois qu'une règle a produit un événement. L'action peut par exemple être le lancement d'un script de remédiation.

5.2.1.4 Cas d'usage

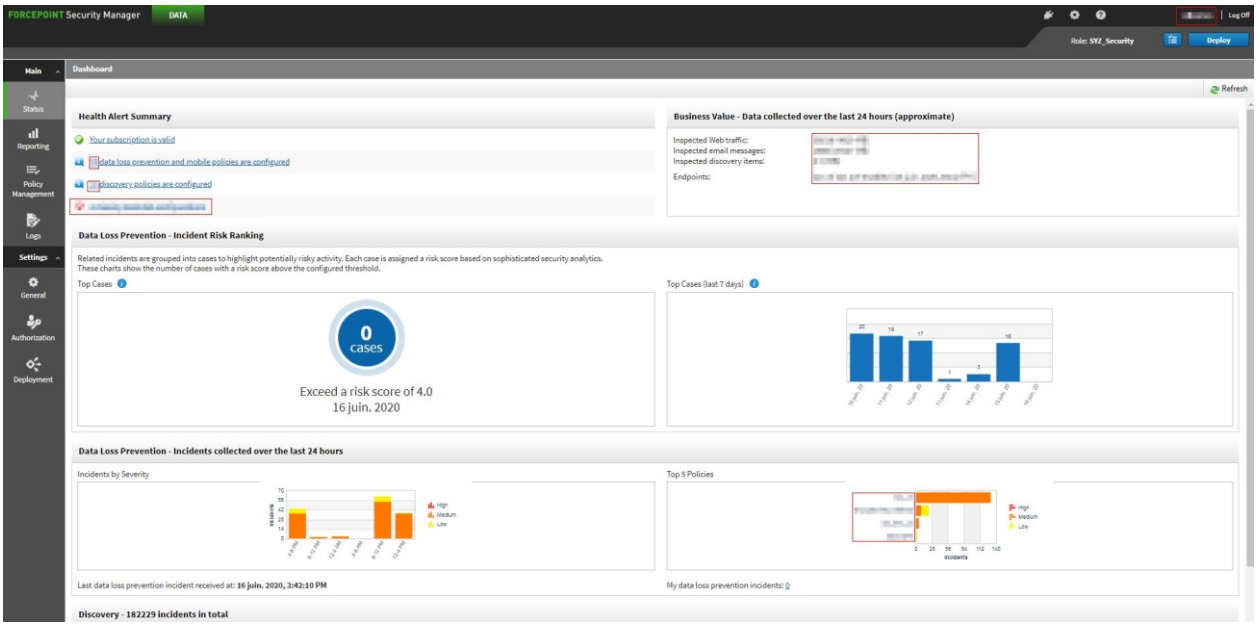
Dans le cadre d'un important transfert de données du Groupe vers un partenaire externe, on a utilisé la fonction DLP Discovery afin de s'assurer que ces données n'étaient pas à caractère confidentiel ou dépendantes du secret des affaires, donc conforme au transfert.

Dans le cas réel, les données confidentielles étaient des CID de type numéro de compte bancaire, nom et prénom de client. Donc, le référentiel de recherche est un extrait de la base de données

clients. Mais, dans ce cas d'usage, pour des raisons de confidentialité, nous allons reproduire le cas réel avec des données fictives, contenant uniquement des faux numéros de compte. Les étapes à suivre pour l'analyse Discovery sont :

- Mise à jour du référentiel de recherche
- Configuration de la règle Discovery
- Paramétrage de l'OCR
- Configuration de la fonctionnalité Discovery
- Gestion des anomalies

Figure 7: Tableau de bord DLP



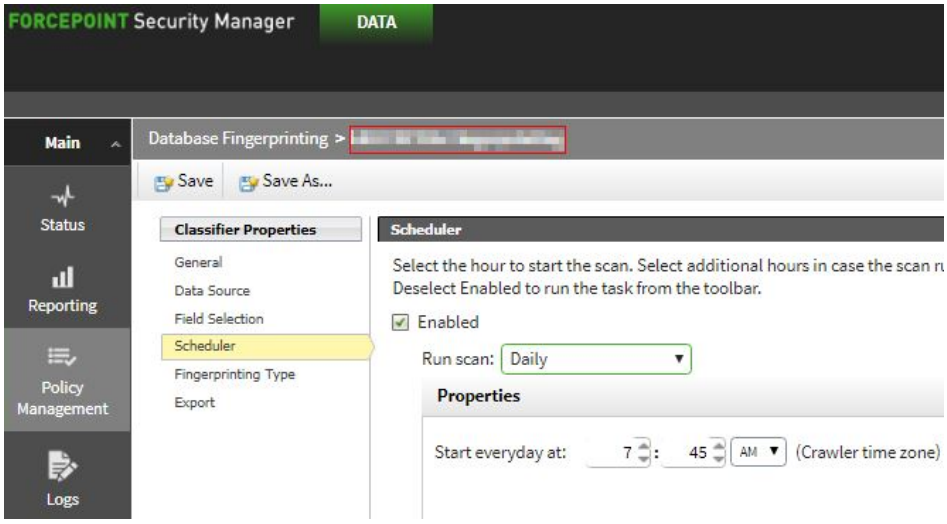
(Christian Djoumessi)

Mise à jour du référentiel de recherche

L'extrait de la base de données est chiffré et intégré dans le DLP, pour en faire une empreinte qui va servir lors des analyses. Notre référentiel est un fichier au format CSV, qui contient une liste de numéros de comptes.

Un point très important lors de la configuration du référentiel, c'est d'automatiser la prise d'empreinte de l'extrait de la base de données à une fréquence définie. Ceci afin de garantir la cohérence des données du référentiel. L'image ci-dessous montre un exemple de prise d'empreinte automatiquement planifié chaque jour à 7h45 AM.

Figure 8: Planification automatique de la prise d'empreinte



(Christian Djoumessi)

Configuration de la règle Discovery

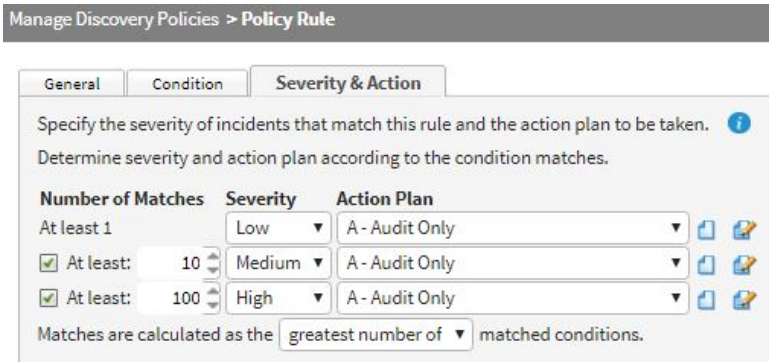
Après avoir configuré le référentiel de données, on va l'utiliser pour la règle Discovery. Notre règle va générer une anomalie dès qu'un numéro de compte est trouvé et l'auditer. Dans la configuration de la règle, on va également prendre en compte les seuils de détection pour définir le niveau de d'importance de chaque anomalie :

- Entre 1 et 9 : Low
- Entre 10 et 99 : Medium
- A partir de 100 : High

Figure 9 : Condition de la règle Discovery

(Christian Djoumessi)

Figure 10: Plan d'action règle Discovery

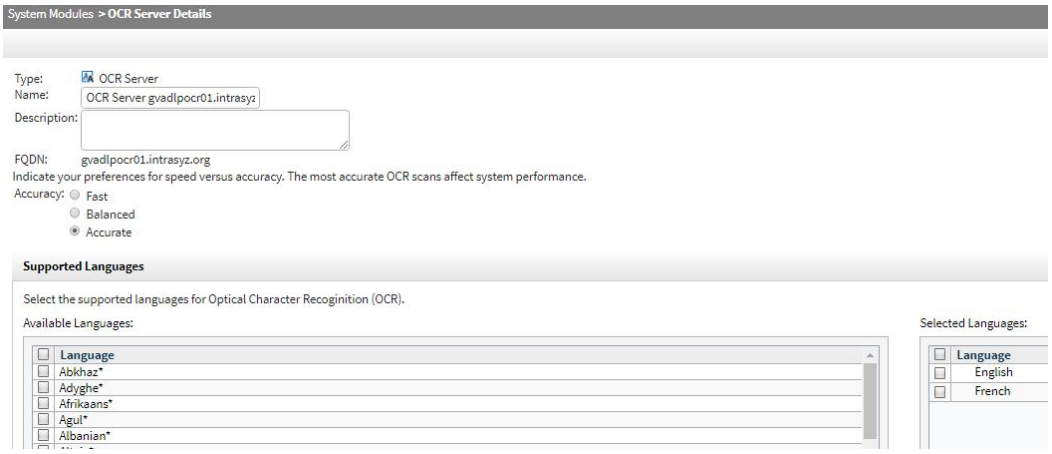


(Christian Djoumessi)

Paramétrage de l'OCR

La fonction du serveur OCR est par défaut prise en compte dans les règles une fois que ce dernier est installé. Afin de pouvoir analyser au mieux les images contenant du texte, il est nécessaire d'adapter la langue de la fonction OCR selon le besoin. Le serveur OCR peut effectuer ses analyses dans plus de 30 langues, mais dans notre cas, on va permettre uniquement le français et l'anglais. Ceci afin d'optimiser l'analyse en réduisant le risque d'avoir des incohérences ; car même avec les langues français et anglais, il en existe toujours. Par exemple la lettre « i », qui en majuscule (« I ») est selon le type de police de caractère utilisé, peut être confondu à « L » en minuscule (« l »).

Figure 11 : Paramétrage de l'OCR



(Christian Djoumessi)

Configuration de la fonctionnalité « Discovery »

Il existe deux sortes de Discovery :

- Endpoint discovery task : tâche d'analyse d'un terminal
- Network discovery task : tâche d'analyse d'un emplacement réseau

Dans notre cas, les données à transférer se trouvent dans un emplacement réseau. Nous allons spécifier le chemin vers l'emplacement (répertoire) à analyser et le compte qui a les droits sur ces données. Pour être sûr de toujours atteindre les données, on va utiliser le compte de service DLP. Ce compte est spécial car il a les droits d'accès en lecture sur tous les répertoires et fichiers du système d'information.

On a aussi la possibilité de planifier la date et l'heure à laquelle la tâche sera effectuée, de manière récursive ou une seule fois. La planification est importante car elle nous permet de pouvoir exécuter une tâche automatiquement à une période où l'on sait que les données seront réellement

au repos, par exemple durant le weekend, ou entre 10h du soir et 6h du matin. Durant ces périodes, il y a très peu de trafic dans le réseau, donc les serveurs d'analyse DLP pourront exécuter les tâches avec plus de ressources CPU.

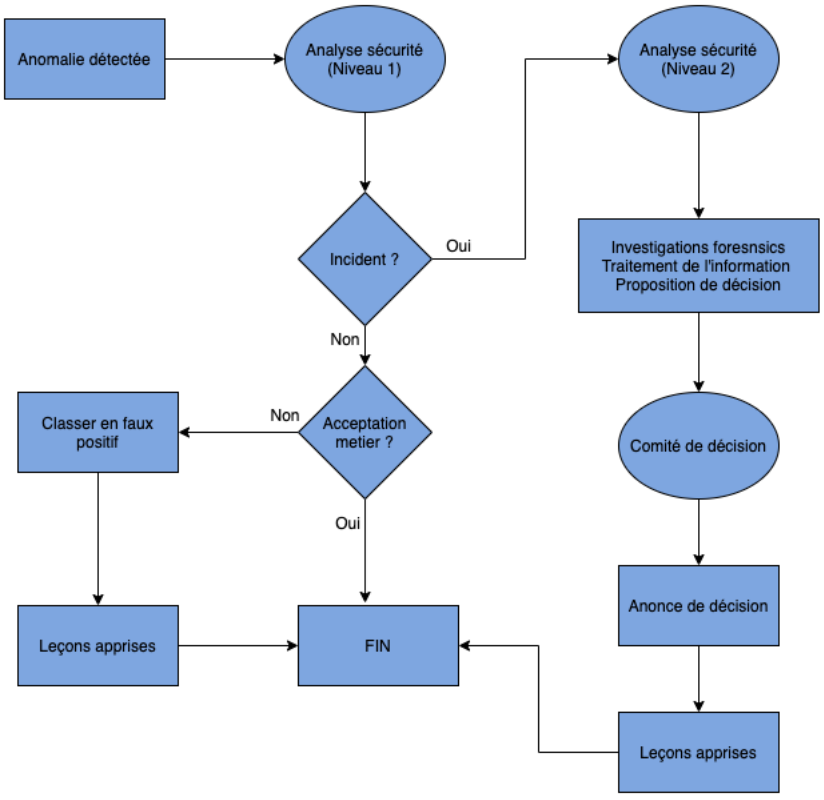
Enfin, on configure un rapport automatique, qui sera envoyé par e-mail aux ayants droits. Ce rapport ne contient pas d'informations sensibles, mais uniquement des statistiques et informations permettant d'identifier la tâche.

Gestion des anomalies

Une anomalie est le résultat d'un événement produit et détecté qui va à l'encontre des règles de sécurité définies. Si le résultat de l'analyse d'une anomalie montre que l'événement lié porte réellement atteinte à la sécurité de l'entreprise, alors l'anomalie devient un incident de sécurité et doit être traité selon le processus en vigueur.

Lorsqu'une anomalie est détectée, on doit suivre la procédure de gestion d'anomalies (voir figure 8). Mais notre cas est différent car la tâche Discovery est faite pour s'assurer que des données confidentielles ne seront pas transférées, ce qui nécessite une coopération avec l'entité métier, propriétaire des données. Donc si des données confidentielles sont détectées, l'information est partagée avec le propriétaire des données afin de les exclures.

Figure 12 : Processus de gestion des anomalies



(Mon employeur)

5.2.2 Participation à l'amélioration de règles de détection des fuites de données

5.2.2.1 Documentation des règles (réalisation et préconisation)

Au cours de mon travail de diplôme, le Groupe a exprimé le besoin d'avoir une documentation à jour des règles DLP afin de :

- Clarifier les aspects techniques
- Avoir les détails qui ont permis de mettre en place chaque règle (la raison de la règle, de son utilisation, les décisions à prendre lorsqu'une règle révèle une anomalie)
- Assurer la compréhension des règles par n'importe quel collaborateur
- Garder un historique des règles qui ont été appliqués à un moment donné pour divers contrôles
- L'ajouter comme document additionnel à la directive encadrant la gestion des incidents de sécurité du Groupe
- Remplir une exigence importante des auditeurs internes et externes

Il a été proposé deux types de documentation au Groupe ; la documentation technique et fonctionnelle. Ces propositions ont été validées par le comité de sécurité du Groupe, et a eu pour résultat la fermeture d'un point d'audit important demandé dans le cas d'une mission conjointe de l'audit interne et externe.

La documentation technique recense l'ensemble des règles et la configuration détaillée de chacune d'elle. Il a été proposé d'utiliser le moyen de génération automatique intégré dans Forcepoint DLP pour produire ce document afin de garantir que tous les aspects techniques de chaque règle soient inclus. Cette documentation ne sera accessible que par les administrateurs de la solution DLP.

La documentation fonctionnelle quant à elle recense l'ensemble des règles et donne un aperçu de chacune d'elle, sans toutes-fois aller dans les détails de la configuration. Cette documentation sera accessible par l'audit interne, également les administrateurs de l'outil DLP et toutes autres parties prenantes identifiées selon le besoin. Le Groupe a donc estimé que l'ensemble des fonctions de contrôle peuvent accéder à cette documentation à la demande.

En ce qui concerne la fréquence de production de ces deux documents, il a été proposé de produire ces documents au fil de l'eau (à chaque modification, création ou suppression d'une règle), ce qui a été validée par le comité de sécurité du groupe.

Ces documents étant confidentiels, il a été proposé de les stocker dans un emplacement sécurisé et restreindre les droits d'accès. Également, mettre en place des contrôles sur l'accès et les modifications apportées sur ces documents. Ces contrôles peuvent être mis en place avec l'aide de l'AD et l'outil Varonis DatAlert, module Varonis actuellement utilisé au sein du Groupe. Deux contrôles seront nécessaires :

- Préventif
    - Création de deux groupes de sécurité dans l'AD : Un groupe pour l'accès en lecture seul de la documentation fonctionnelle, et un groupe pour l'accès en lecture et écriture de la documentation technique
    - Création de deux répertoires ; un répertoire par type de document, et assigner les accès et permissions aux répertoires par les groupes de sécurité créés au point précédent
    - Classifier le document comme confidentiel selon la directive de l'entreprise
- Détectif
    - Configuration des alertes Varonis pour chaque accès, tentative d'accès et écriture dans les répertoires créés. Les alertes seront envoyées par e-mail à l'équipe en charge de la sécurité du système d'information
    - Mise en place d'une règle DLP basée sur la classification des documents

Les anomalies qui seront générées par les contrôles détectifs seront prises en charge par l'équipe sécurité pour investigations.

5.2.2.2 Implémentation de nouvelles règles et optimisation

Dans les organisations, il existe des règles de sécurité standards même au sens DLP qui sont globales indépendamment du secteur d'activité. Mais en général, les règles de sécurité sont faites sur mesure et selon le fonctionnement de chaque organisation.

Une des difficultés auxquelles les équipes de sécurité sont confrontées est le traitement d'énormes quantités d'anomalies de sécurité, dans lesquelles il existe plusieurs faux positifs. Dans les cas du Groupe, les ressources humaines ne sont pas assez nombreux pour gérer la quantité d'anomalies générées par le DLP. Ce qui augmente considérablement le risque de ne pas être en mesure de traiter les anomalies pertinentes, qui pourraient être de réels incidents de fuite de données avec des impacts sur l'entreprise comme on l'a décrit dans le chapitre 3 de ce document.

Après analyse des anomalies DLP, nous avons pu détecter plusieurs faux positifs réguliers. L'action suivante était de regrouper les anomalies par leurs éléments en commun (par exemple la source et la destination des événements) et définir une règle d'exception basée sur ces éléments en commun.

Comme cas concret, nous avons par exemple identifié qu'une unité métier de gestionnaires de portefeuilles échangeait régulièrement via e-mail avec des partenaires gérants indépendants. Ces échanges contenaient des CID. Du point de vue sécurité, cela représente une anomalie et potentiellement un incident. Tandis que du point de vue métier, c'est un comportement normal. Nous avons donc mené un travail avec l'entité en question, afin de déterminer tous les partenaires avec qui leurs échanges contiennent des CID. Ce travail nous a permis de définir une règle d'exception pour cette unité en prenant en compte toutes les informations collectées. Ce

processus a porté ses fruits et a été validé par le comité de sécurité pour son application avec d'autres unités métier identifiés. Ce processus permet de :

- Ne pas impacter les activités du métier
- Réduire le nombre de faux positifs
- Avoir une meilleure visibilité des anomalies
- Se concentrer sur les cas importants

5.2.2.3 Tests des règles nouvellement implémentées

Dans ce sous chapitre, nous allons prendre comme exemple l'optimisation décrite dans le sous-chapitre précédent, c'est-à-dire mettre en place une règle qui analyse les CID, et une exception selon les informations métiers. Pour ce faire, nous allons utiliser des données fictives pour des raisons de confidentialités.

Pour cet exemple, les paramètres à prendre en compte sont les suivantes :

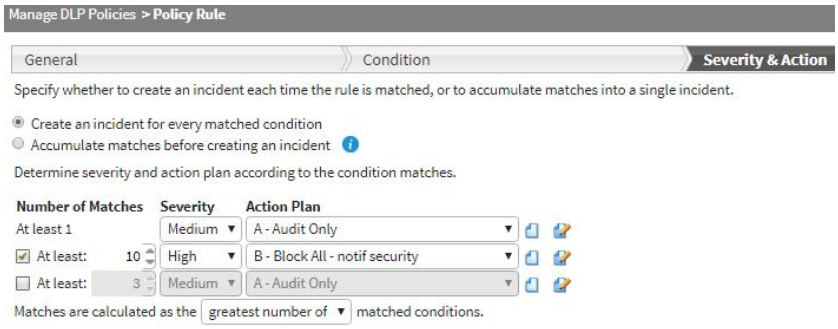
- Auditer les envois de 0 à 9 numéros de compte sur tous les canaux DLP
- Bloquer les envois de plus de 9 numéros de compte (considérons que l'envoie de plus de 9 numéros de compte est un envoi massif de CID) sur tous les canaux DLP
- Si l'adresse e-mail de destination est une adresse de la HEG Genève ou n'importe quelle HES-SO, et la source est un collaborateur du département sécurité, alors c'est un comportement normal du métier ; l'envoi de plus de 9 numéros de compte est autorisé et n'est pas audité

Avec ces trois informations, nous allons mettre en place les éléments nécessaires à la création de la règle DLP et ensuite la créer, en suivant ces étapes :

- Créer une « Business Unit » nommée « Test_Security » et y ajouter les collaborateurs du département sécurité
- Créer un référentiel de données de type dictionnaire nommé « Test_HES_Domains » et y ajouter le nom de domaine de la HEG Genève « hesge.ch »
- Créer la police et la règle DLP qui audite ou bloque le trafic selon les recommandations. Nous allons les nommer « T_HEG » (dont T signifie test)
- Créer la règle d'exception nommée « T_E_HEG » (dont E signifie exception) selon les recommandations

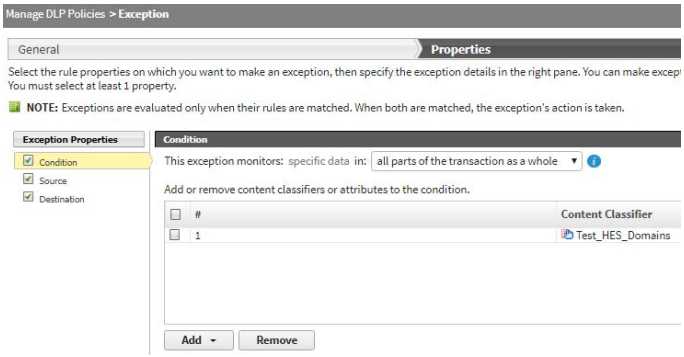
Supposons que la « Business Unit », le dictionnaire et la condition de la règle (voir la figure 8) sont déjà créés, et passons à la création de la règle DLP. Les figures suivantes montrent le plan d'action à mettre en place pour la règle DLP et la règle d'exception configurée.

Figure 13: Plan d'action règle DLP



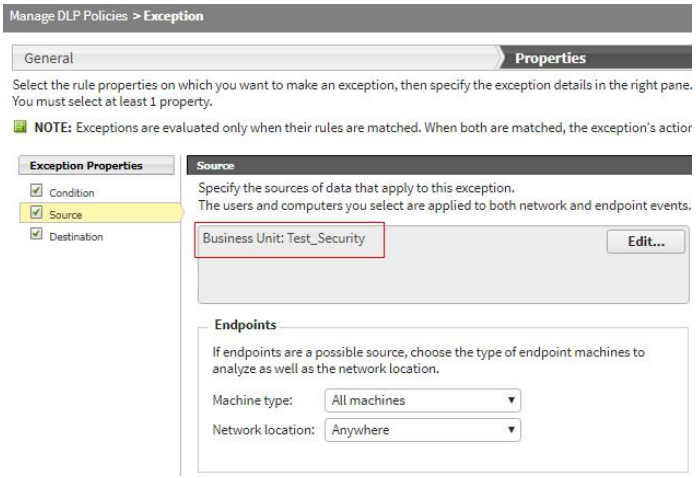
(Christian Djoumessi)

Figure 14: Condition de la règle d'exception



(Christian Djoumessi)

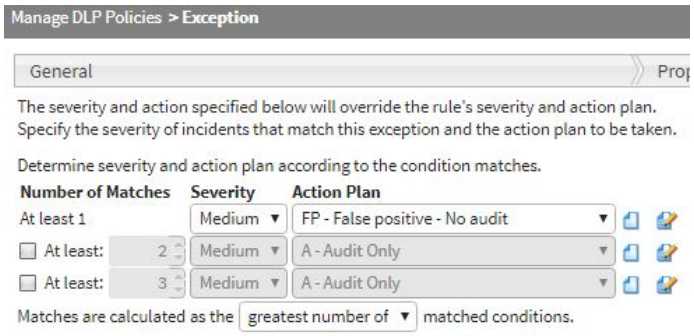
Figure 15: Source de l'exception



(Christian Djoumessi)

La figure suivante montre le plan d'action de la règle d'exception (ne pas auditer l'événement), mais dans notre cas de test, afin de visualiser dans la console de management DLP que ce type d'événement n'a pas été bloqué, nous allons l'auditer.

Figure 16: Plan d'action de la règle d'exception



(Christian Djoumessi)

Le tableau suivant montre les tests qui ont été effectués ainsi que les résultats :

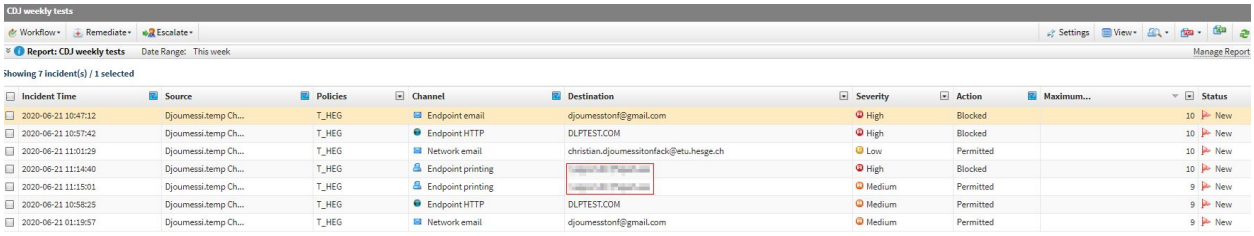
Tableau 2: Tests DLP effectués

Description du test	Résultat
Envoi d'un e-mail contenant 9 numéros de compte à une adresse gmail.com	Autorisé
Envoi d'un e-mail contenant 10 numéros de compte à une adresse gmail.com	Bloqué
Envoi d'un e-mail contenant 10 numéros de compte à une adresse etu.hesge.com	Autorisé
Upload de 9 numéros de compte à l'adresse dlptest.com	Autorisé
Upload de 10 numéros de compte à l'adresse dlptest.com	Bloqué
Impression d'un document contenant 9 numéros de compte	Autorisé
Impression d'un document contenant 10 numéros de compte	Bloqué

(Christian Djoumessi)

L'image suivante de la console de management illustre les résultats des tests du tableau 2 :

Figure 17: Rapport des tests DLP



(Christian Djoumessi)

5.2.3 Contribution à la gestion des incidents

De nouveaux types d'incidents de sécurité émergent fréquemment. De ce fait, le Groupe doit être préparé à faire face aux événements de sécurité connus ou inattendues. Pour assurer cette préparation qui permettra de réduire le nombre d'incidents de sécurité, des éléments de

préventions, détections et réponses basés sur les résultats d'évaluation des risques doivent être adressés. Il est quand même à noter que pas tous les incidents de sécurité peuvent être évités.

Le Groupe poursuit le projet nommé ISIR (Information Security Incident Response) qui a pour objectif de décrire et mettre en place un cadre pour répondre aux incidents de sécurité. Actuellement à la phase de documentation, ISIR définit :

- Les caractéristiques des incidents de sécurité
- Les six phases de réponses aux incidents
- Les cas d'utilisations et manuel de réponse[7] aux incidents de sécurité
- Les différents rôles et responsabilités

5.2.3.1 Revue du processus de la gestion des incidents DLP

En se basant sur les référentiels du SANS et NIST, un top 10 des incidents de sécurité a été défini et pour chaque type d'incident, un manuel de réponse sera établi. Le top 10 identifié de types d'incidents est le suivant :

- Ingénierie sociale
  - Pratique de manipulation incitant la victime à fournir des informations
- Actif compromis
  - Tels que des équipements réseaux et mobiles de l'entreprise, qui sont exploités par une personne malicieuse avec comme résultat une perte de la confidentialité, l'intégrité ou la disponibilité
- Fuite de données
  - Mouvement non-autorisé des données généralement vers l'extérieur de l'entreprise. Par exemple des CID et documents stratégiques sensibles
- Déni de service
  - Attaque ayant pour objectif de rendre un service indisponible
- Destruction/perte d'actif
- Accès non-autorisé
  - Aussi référé comme une intrusion
- Attaque zero-day[8]
- Informations d'identification compromises
- Attaque par défiguration[9]

[7] Le terme en anglais « framework » est généralement utilisé

[8] Une attaque de type zero-day est une cyberattaque ciblée exploitant une vulnérabilité de sécurité d'un logiciel avant la mise à disposition d'un correctif par l'éditeur du logiciel

[9] L'attaque par défiguration est une cyberattaque exploitant une vulnérabilité connue et non-corrigé d'un site web, au cours de laquelle l'attaquant ajoute du contenu dans la page web

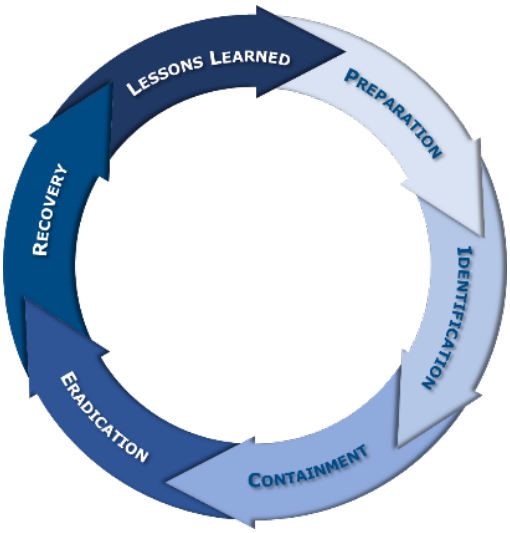
- Violation de politique de sécurité

Le Groupe a basé son plan de réponse aux incidents de sécurité sur le modèle à six phases du SANS, qui sont :

- Préparation
  - Cette phase inclut les tâches qui doivent être exécutées afin de se prémunir ou éviter l'occurrence d'un incident de sécurité, ou de limiter son impact
- Identification
  - C'est la phase de reconnaissance d'un incident. Les incidents sont soit remontés par les utilisateurs finaux soit détectés par le SIEM et d'autres outils de détection
- Endiguement
  - Dans cette phase on met en place des moyens afin de limiter les dommages causés par un incident
- Éradication
  - Le but de cette phase est de mettre en marche le plan de remédiation suite à l'endiguement, et de restaurer les systèmes affectés
- Récupération
  - Dans cette phase on remet les systèmes affectés en production, une fois restaurés
- Leçons apprises
  - L'une des phases les plus importantes ; son but est de finaliser la documentation de l'incident, fermer l'incident et déterminer les plans d'actions pour améliorer le processus de gestion d'incidents

Toutes ces phases représentent un cycle continue dans lequel le traitement de chaque événement de sécurité se termine toujours par de leçons apprises. La revue de ce processus se fait deux fois par an et est à la responsabilité du CISO du groupe, en collaboration avec les TISO.

Figure 18: Processus de réponse aux incidents



(Mon employeur)

5.2.3.2 Processus d'amélioration du traitement des incidents (préconisation)

Le Groupe a mis en place une matrice RACI afin de déterminer les rôles et responsabilités des parties prenantes pour les tâches liées aux six phases du processus de gestion. Cette matrice se trouve à l'annexe 3. Mais tout d'abord, il est important de comprendre ce qu'est une matrix RACI. Il s'agit d'un tableau à deux dimensions contenant les tâches, et les quatre rôles suivants :

- R : Réalise ; celui qui est responsable ou qui effectue la tâche
- A : Approuve ; celui qui supervise la tâche
- C : Consulté ; celui qui consulte la tâche et donne ses opinions ou conseils
- I : Informé ; celui qui est tenu à jour de l'avancé de la tâche

Dans la matrice RACI de l'annexe 3, nous constatons que la partie prenante IRT participe énormément en tant que responsable dans la phase d'identification des incidents. Afin d'avoir une meilleure ségrégation des responsabilités, il a été proposé d'ajouter une nouvelle partie prenante appelé « Security Analyst », qui prendra en charge la responsabilité de l'IRT de la phase identification. Le « Security Analyst » aura également la responsabilité d'assigner les incidents aux personnes appropriées, et les TISO seront informés de cette tâche. Cette ségrégation de rôles permettra notamment à l'IRT de se concentrer sur les tâches d'endiguement, d'éradication et de récupération car comme nous avons noté dans chapitre 5.2.2.2, les équipes de sécurités font très souvent face à d'énormes quantités d'événements de sécurité, et il est très important de pouvoir rapidement éradiquer un incident afin de limiter l'impact que ça peut avoir au métier.

5.3 Gestion des risques externes

Les risques externes, aussi appelés risques exogènes, sont essentiellement constitués de situations provenant de l'extérieur de l'organisation concernée et qui peuvent la mettre en péril. En sécurité informatique, le risque externe est directement lié aux menaces extérieures auxquelles les systèmes d'information sont exposés.

5.3.1 Étude des éventuels contrôles DLP dans un environnement cloud

Enjeux du cloud

Les enjeux du cloud pour les entreprises à ce jour restent énormes, et nous allons nous concentrer sur ceux susceptibles d'impacter les instituts financiers. Une analyse de risques liés au cloud a été effectuée et il en découle des risques portant notamment sur :

- La confidentialité : Manque de contrôle d'accès aux données
- Intégrité : Comme nous ne maîtrisons pas correctement l'accès aux données, nous ne pourrons pas garantir que les données ne sont pas altérées

Il est à noter que la disponibilité n'est pas un problème car les fournisseurs de services cloud disposent de moyens adéquats pour assurer ce volet.

Analyse de risque global

Les instituts financiers se penchent souvent sur les facteurs de risque suivants, pour lesquels nous avons fait une analyse (voir l'annexe 2 pour les échelles d'évaluations des risques):

Tableau 3: Analyse des risques cloud

ID	Risques identifiés	CIA[10]	Applicable au Groupe (O/N)	Occurrence	Impact	Niveau de risque	Mitigation	Risque résiduel
1	Accès non autorisé aux données confidentielles	C	O	Possible	Catastrophique	Haut	Rapports automatiques sur l'accès aux données sensibles, revue périodique des permissions utilisateurs	Bas
2	Défaut de protection de données	C	O	Rare	Modéré	Bas	Maintenir les données sensibles sur site	Bas
3	Mauvaise configuration des rôles	C	O	Possible	Catastrophique	Haut	Revue périodique des rôles et permissions	Moyen
4	Manque de contrôle d'accès basé sur les rôles	C	O	Possible	Catastrophique	Haut	Maintenir le processus d'autorisation sur site	Moyen
5	Modification des données inattendues ou non-contrôlé	I	O	Rare	Modéré	Bas	Mettre en place un processus de gestion de changement, mettre en place des KPI/KRI pour vérifier cette mise en place, audit périodique des changements, maintenir le processus d'autorisation sur site, imposer au prestataire les rapports ISAE3402/3000 sur ce risque	Bas
6	Perte de sauvegarde et récupération	I	O	Possible	Majeur	Haut	Redondance des sauvegardes sur avec d'autres fournisseurs cloud, demander des rapports de tests « Disaster Recovery », réduire le « Recovery Point Objective (RPO) »	Bas

[10] C: Confidentiality, I: Integrity, A: Availability

7	Perte d'appartenance de données	I	O	Probable	Modéré	Haut	Utilisation de services et communauté de type threat intelligence (digital shadow, MELANI[11], FS-ISAC[12], MISP[13])	Moyen

(Christian Djoumessi)

L'annexe 2 présente les échelles d'évaluation des risques et les codes couleurs utilisés dans le tableau précédent.

Le Cloud Security Alliance a fait une étude afin de définir des moyens de contrôle de sécurité face aux risques cloud. Dans l'annexe 1, nous avons associé ces contrôles adressés aux différents risques de notre analyse.

DLP Cloud

Le Groupe a déjà commencé son développement sur le cloud, avec une entité ayant son système d'information sur le cloud. Le DLP Cloud permet d'adresser un contrôle sur la fuite de données vers le cloud. Ayant déjà en place l'outil DLP Forcepoint pour l'infrastructure sur site, nous avons mené une étude sur son module DLP Cloud qui permet de couvrir une partie de l'aspect CASB, appelé Forcepoint DLP Cloud Application. Ce module a les avantages suivants :

- Intégration avec l'architecture DLP sur site
- Contrôle de fichiers déposés sur les applications cloud (données en mouvement)
- Découverte et remédiation de données sensibles stockées sur le cloud (DLP Cloud Data Discovery)
    - Plan de remédiation possible allant de la suppression des droits de partage à la mise en quarantaine
- Anomalies générées et « forensiques » stockées sur l'infrastructure sur site et non sur le cloud
- Plusieurs applications cloud supportées à ce jour parmi lesquelles figurent :
    - Office 365
    - Box
    - G-Suite
    - Salesforce

[11] Centrale d'enregistrement et d'analyse pour la sûreté de l'information

[12] Centre d'analyse et de partage d'informations sur les services financiers

[13] MISP (Malware Information Sharing Plateform) est une solution applicative open source de renseignement sur les menaces informatiques

- ServiceNow

Très utilisée en entreprise, la classification des données par des labels permet de déterminer le niveau de confidentialité de celles-ci. Forcepoint DLP Cloud Application intègre le module « Data Labeling Framework » qui permet de :

- Automatiquement appliquer des labels sur les données au repos. Les labels possibles sont :
  - Titus labeling solutions
  - Microsoft Information Protection
  - Bolden James classifier
- Détecter des labels avec les règles DLP

5.3.2 Initiation au SIEM

Nous avons décrit dans le chapitre 5.1.2 l'outil d'analyse de log, qui est la solution SIEM utilisée par le groupe. Le groupe a été confronté à une problématique adressant le risque d'indisponibilité des services DLP. La problématique était la suivante ; un changement effectué sur une base de données, a rendu les services DLP indisponibles pendant plusieurs jours, ce qui a eu comme effet le non-contrôle des communications sortantes en SMTP et Web. Nous verrons dans le sous-chapitre suivant le contrôle qui a été mis en place afin de réduire ce risque.

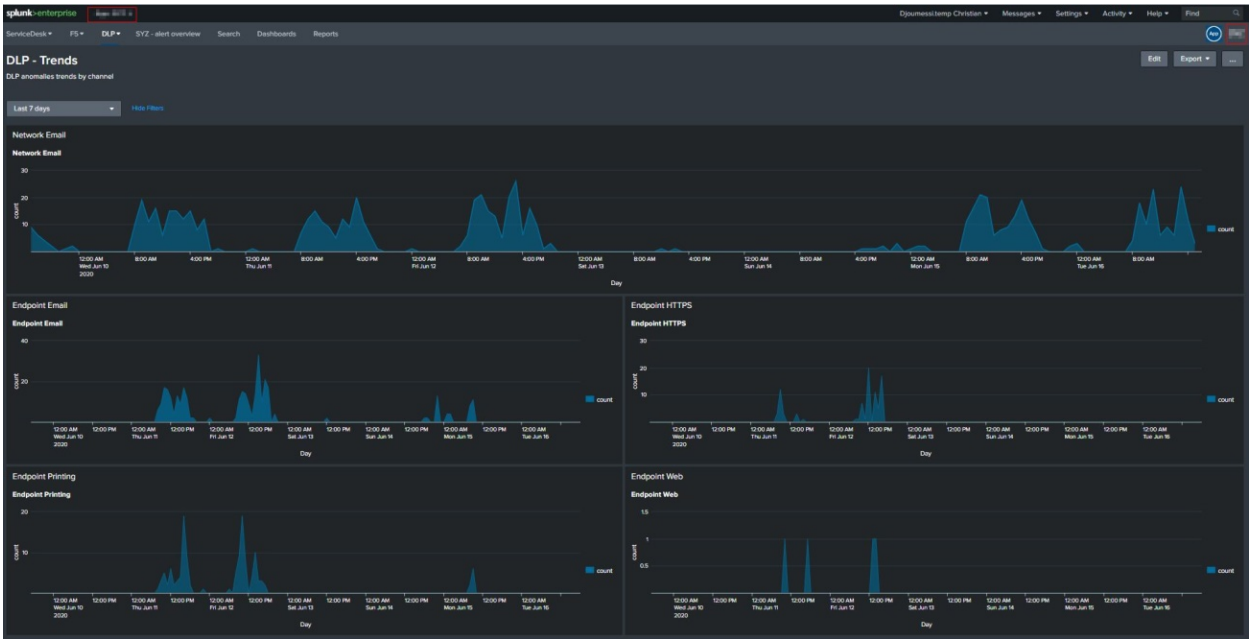
5.3.2.1 Mise en place d'un tableau de bord pour la disponibilité des serveurs critiques

Suite au risque exposé précédemment, il a été mis en place un tableau de bord sur Splunk qui permet d'avoir un visuel en temps réel des anomalies détectées, sur les canaux :

- SMTP
- Web
- Imprimante

Il est possible de modifier la plage de temps et définir la période voulue de récolte d'informations. Sur la figure ci-dessous, on peut par exemple constater que le canal SMTP est celui qui génère le plus de trafic. Pratiquement chaque heure (hormis pendant la pause de midi et entre 6h du soir et 8h du matin) durant les jours ouvrés, des anomalies sont générées. S'il y a aucun trafic sur le tableau de bord pendant plusieurs heures, on pourrait directement se poser la question quant à la disponibilité des services DLP, et faire des investigations.

Figure 19 : Tableau de bord DLP - Trends



(Christian Djoumessi)

5.4 Revalidation des accès

Pour faire fuiter des données, il faut déjà y avoir accès. C'est pourquoi la gestion des accès dans un système d'information est un élément important contre la fuite de données. Ceci passe par une gouvernance des données concernant notamment la façon dont les données sont stockées, l'attribution des bons droits d'accès aux utilisateurs, et ensuite la revalidation des accès afin de s'assurer qu'avec les modifications organisationnelles dans l'entreprise qui varie dans le temps, les bons droits d'accès restent attribués de manière optimum. A savoir que les bons droits d'accès relèvent du principe du moindre privilège.

Annuellement, le Groupe conduit une campagne interne de revalidation des accès aux répertoires et applications sensibles. Ceci afin de couvrir les contrôles basés sur la circulaire FINMA 2008/21 annexe 3 qui sont mis en avant dans le rapport annuel ISAE 3402[14]. Ces contrôles sont les suivants :

- Les droits d'accès ne sont attribués qu'aux utilisateurs actifs au sein du groupe (employés et consultants)
- Les accès aux données ou fonctionnalités sont attribués aux utilisateurs uniquement quand il est nécessaire pour l'exécution de leurs tâches (principe du moindre privilège)
- Les permissions doivent être confirmées annuellement

[14] ISAE (International Standards for Assurance Engagements) 3402 : Rapport d'assurance sur les contrôles dans une entreprise de service

Ces contrôles permettront d'assurer que les droits d'accès adéquats sont attribués aux bons rôles métiers. Autres fois, la campagne se déroulait manuellement. Les managers recevaient un document, contenant la liste des répertoires et applications dont ils étaient responsables et les accès à ces derniers. Présentement, la revalidation des accès aux répertoires se fait avec l'outil de gouvernance des données Varonis DataPrivilege.

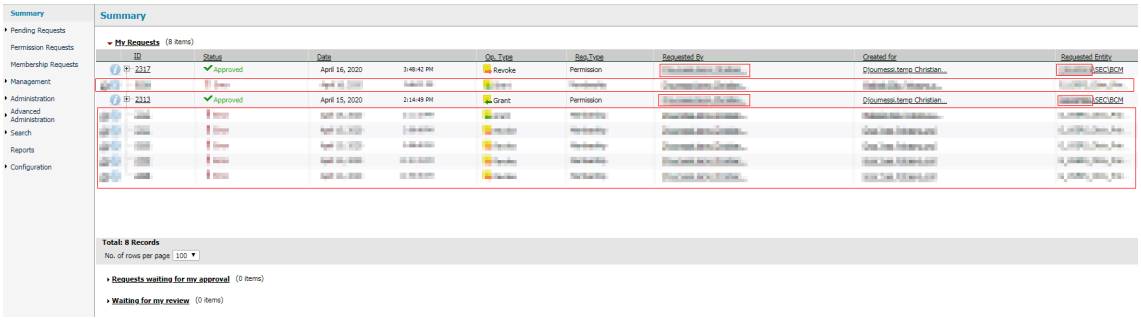
5.4.1 Configuration de l'outil de supervision pour la revalidation des accès

5.4.1.1 Présentation de l'outil Varonis DataPrivilege

Varonis est un éditeur américain spécialisé dans les outils de gouvernance des données structurées et non-structurées. DataPrivilege est un module du panel d'offre de Varonis qui sert à la gouvernance de l'accès aux données.

Cet outil permet de vérifier la conformité des droits d'accès au travers des campagnes de revalidation d'accès et aussi de mettre en place un modèle de moindre privilège en donnant aux utilisateurs propriétaires de données les moyens de modifier et gérer les droits des dossiers, sites SharePoint et groupes AD (Active Directory) sans l'intervention du département informatique. Aucun droit administrateur n'est requis. Une fois toutes les autorisations obtenues, DataPrivilege gère toutes les modifications en arrière-plan et de façon transparente.

Figure 20: Varonis DataPrivilege



(Christian Djoumessi)

5.4.2 Campagne de revue des accès aux applications critiques

5.4.2.1 Rétrospective de la dernière campagne

Sous le contrôle du CISO du groupe, la campagne de revalidation des accès aux applications critiques s'est déroulée pendant 3 mois.

Contrairement à la revalidation des accès aux répertoires comme nous allons voir par la suite, il n'y a pas de notion de propriétaire de données (« data owner »). Pour certaines applications, il existe deux niveaux de validations ; responsable d'application et responsable de service.

Le résultat de la campagne a produit les informations suivantes :

- 132 applications concernés par la campagne

- 23 responsables d'applications
- 19 responsables de services
- 97% de la revue a été effectuée

5.4.2.2 Points d'amélioration

A la fin de la campagne, les remarques suivantes ont été énoncées :

- En ce qui concerne l'inventaire des applications, la cartographie des services (liste des applications et responsables de chaque) doit être mise à jour
- Une approche commune concernant l'évaluation de la criticité (présence des CID, données personnelles, données stratégiques, etc) des applications doit être mise en place
- Une cohérence des informations RH des employés versus les informations de l'AD doit être mis en place

Varonis DataPrivilege peut nous permettre d'automatiser une partie de cette campagne. Pour cela, il faudrait faire une étude afin d'identifier les applications qui n'ont qu'un niveau de validation et pour qui les utilisateurs sont gérés via des groupes de sécurité. De la même façon dont nous avons tenu la campagne de revalidation aux répertoires sensibles (voir le sous-chapitre suivant), nous pourront faire pareil en appliquant la notion de responsable de groupe de sécurité, qui pourrait correspondre au responsable d'application.

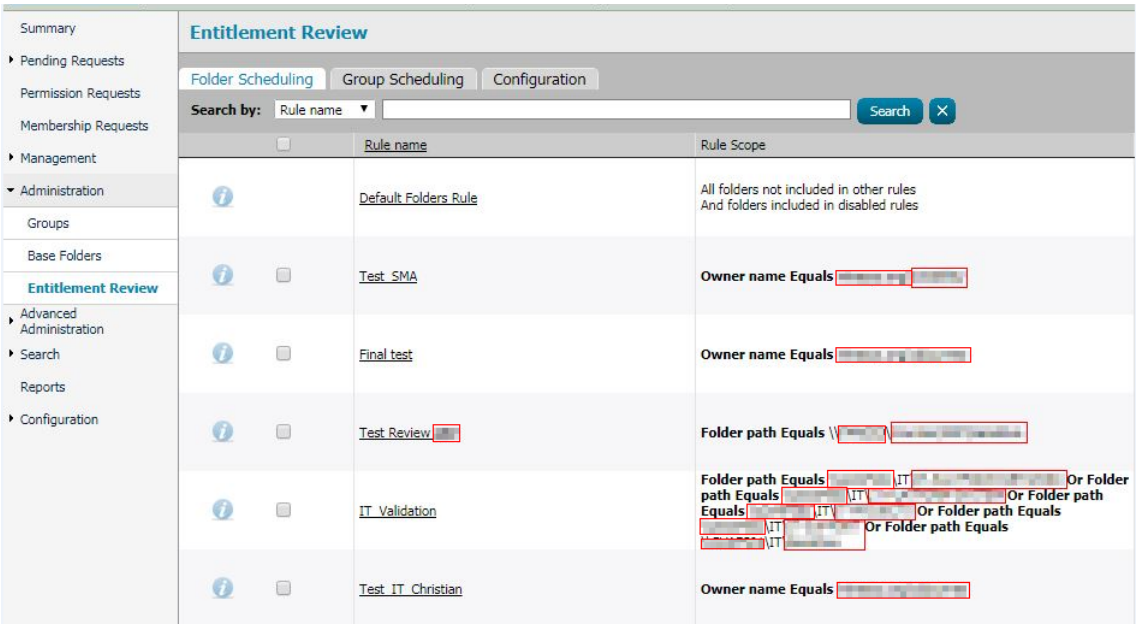
5.4.3 Campagne de revue des accès aux répertoires sensibles

5.4.3.1 Rétrospective de la dernière campagne

La dernière campagne s'est tenue pendant 2 mois. Avant la campagne, plusieurs tests de la procédure de revue des accès ont été effectués, dans un premier temps avec l'IT et dans un deuxième avec une partie du métier (trading et opérations). Ces tests avaient pour but de se rassurer du bon fonctionnement de l'outil et aussi de la bonne compréhension des utilisateurs métiers (responsables des données) concernés par la campagne, sur la façon d'effectuer la campagne.

La figure suivante montre une partie des règles de tests de la revalidation des accès. Pour des raisons de confidentialité nous n'allons pas entrer dans les détails des règles. Mais il est à noter que lors de la configuration d'une règle, on paramètre la date et l'heure à laquelle la règle sera exécutée automatiquement. Une fois la règle exécutée, les propriétaires des données reçoivent un e-mail contenant toutes les indications nécessaires pour effectuer la campagne.

Figure 21: Revalidation des accès aux répertoires sensibles



(Christian Djoumessi)

Les périmètres des répertoires concernés par la revue des accès étaient les suivants :

- Répertoires chiffrés
- Répertoires de service
- 99% de la revue a été effectuée.

A la fin de la campagne, nous avons remarqué les anomalies suivantes :

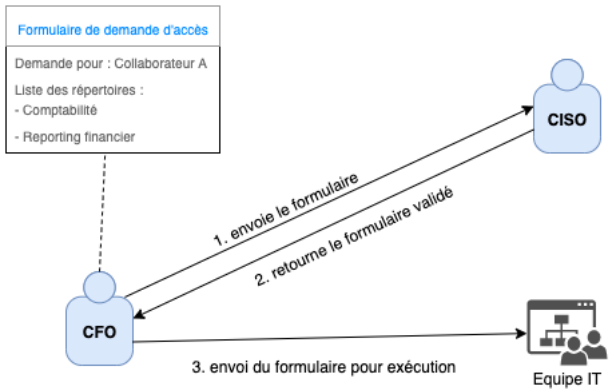
- Certains managers ont demandé d'ajouter des droits d'accès aux répertoires pour certains collaborateurs
- Les comptes de plusieurs collaborateurs ayant quitté l'entreprise avaient encore des droits d'accès à certains répertoires

Améliorer le processus de gestion des accès mènerait à ne plus avoir ces anomalies citées plus haut.

Prenons le cas de l'arrivé d'un nouveau consultant. La situation actuelle d'attribution des droits d'accès aux répertoires suit le workflow suivant :

- Le manager remplit un formulaire papier dans lequel il spécifie les accès du consultant et l'envoie à la sécurité pour validation
- L'équipe sécurité valide la demande et le renvoie au manager
- Le manager envoie sa demande validée par la sécurité à l'équipe IT pour exécution
- L'équipe IT configure les accès

Figure 22: Processus d'attribution des accès actuel



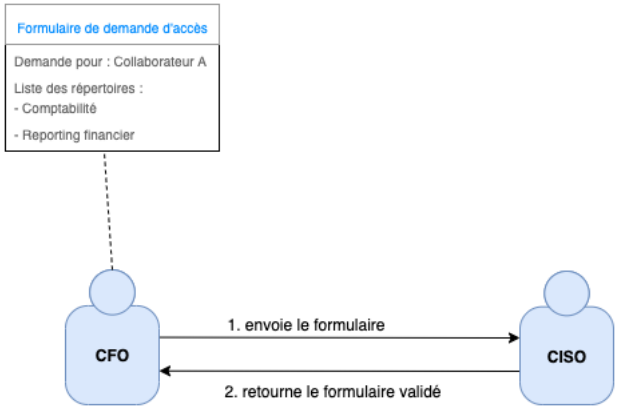
(Christian Djoumessi)

Dû au fait que les managers sont à même de valider les accès aux répertoires de leurs collaborateurs lors de la campagne de revue des accès, pourquoi ne pas ne les rendre apte à donner et éventuellement retirer directement ces droits aux collaborateurs quand cela est nécessaire ?

5.4.3.2 Amélioration de la gestion des accès

L'amélioration de la gestion des accès aux répertoires se basera sur le principe de moindre privilège. Dans la figure précédente, on peut constater que l'équipe IT n'a pas forcément besoin de connaître au préalable les accès qu'aura un collaborateur. Donc, cette l'information peut se limiter entre le département sécurité et le propriétaire des données, et la tâche opérationnelle revient au propriétaire des données.

Figure 23: Processus d'attribution des accès amélioré



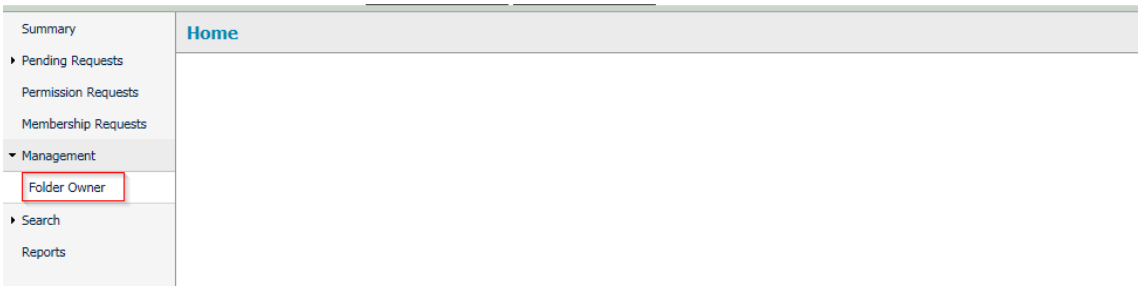
(Christian Djoumessi)

Dans ce cas de figure, le propriétaire des données va procéder à la configuration des droits d'accès via l'interface web Varonis DataPrivilege, et cette configuration sera appliquée en arrière-plan par le compte de service Varonis.

Dans le système d'information du Groupe, la configuration des droits d'accès via Varonis se fait par les étapes suivantes :

Dans le navigateur web, ouvrir le lien https://varionis.banque.org/[15]

Figure 24: Synthèse des demandes



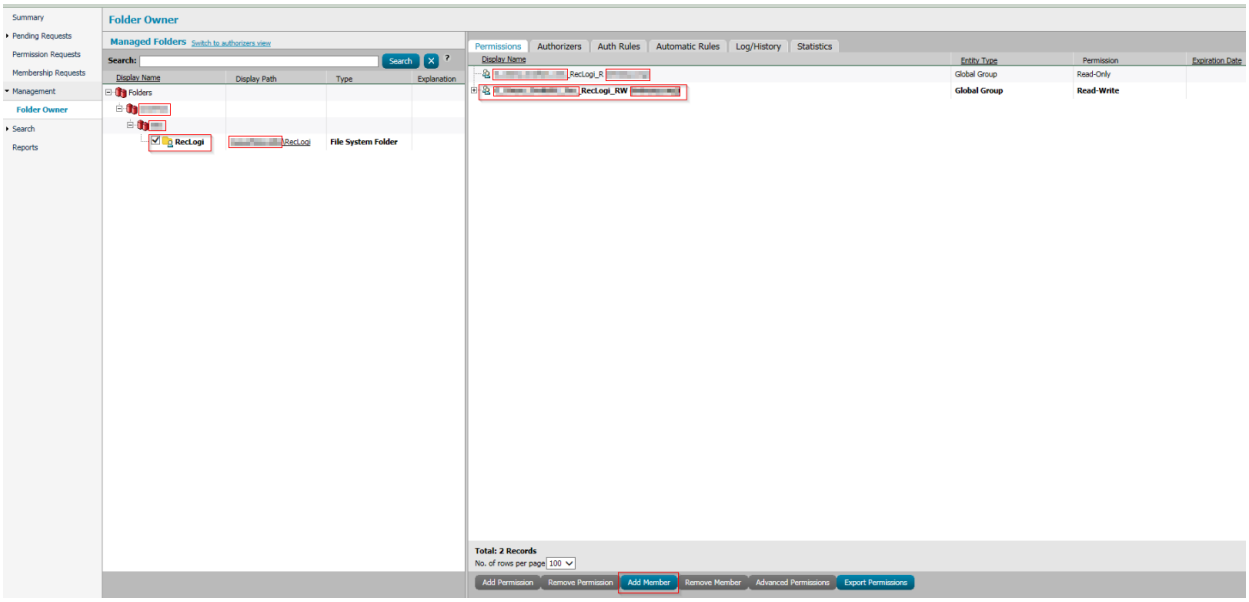
(Christian Djoumessi)

Dans la page d'accueil, sous le menu Management, sélectionner « Folder Owner ». Dans la page qui s'affiche, sélectionner un répertoire et dans l'onglet « Permissions », sélectionner un groupe, et ensuite cliquer sur « Add Member ». Il est à noter que chaque répertoire a deux groupes d'accès associés :

- Le premier avec le nom se terminant par « R » pour dénoter la permission en « Read », donc lecture seule
- Le second avec le nom se terminant par « RW » pour dénoter la permission en « Read-write », donc lecture et écriture

[15] Ceci est une adresse internet fictive à titre indicatif

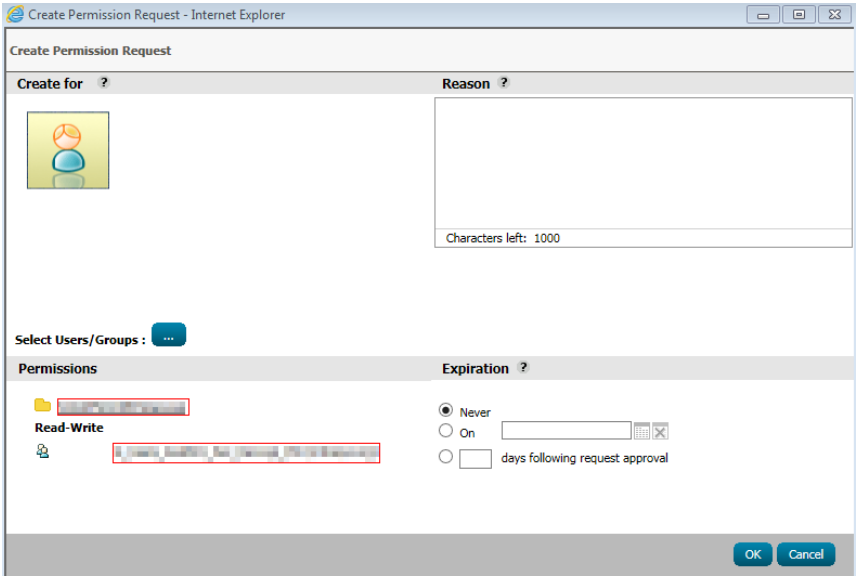
Figure 25: Droits d'accès et permissions



(Christian Djoumessi)

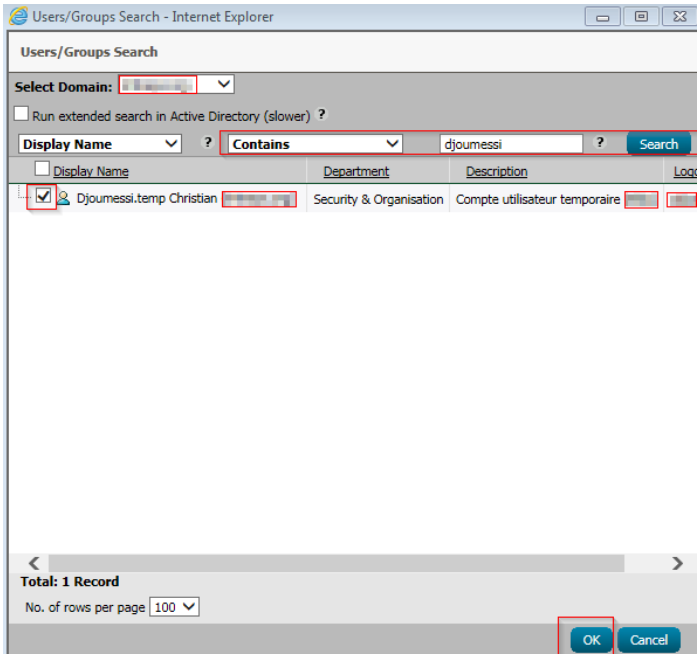
Dans la fenêtre qui s'ouvre, cliquer sur le bouton bleu de « Select Users/Groups » afin de rechercher l'utilisateur.

Figure 26: Création d'une permission



(Christian Djoumessi)

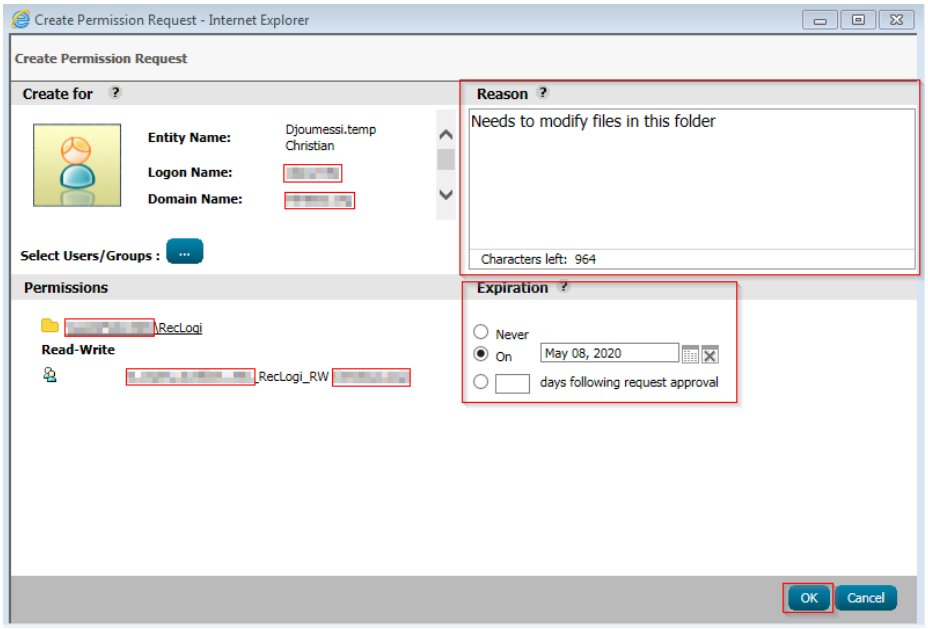
Figure 27: Sélection des utilisateurs liés à la création de la permission



(Christian Djoumessi)

Enfin, entrer une raison de l'attribution des permissions et déterminer la date d'expiration de ces accès. Arrivé à la date paramétrée, les permissions seront automatiquement révoquées à l'utilisateur.

Figure 28: Confirmation de la création de la permission

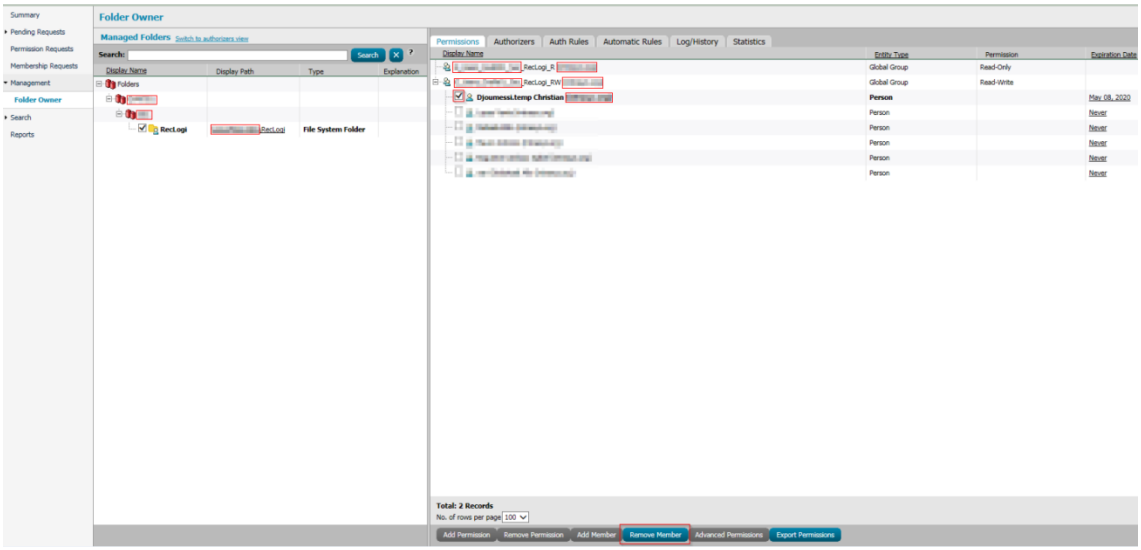


(Christian Djoumessi)

L'utilisateur obtient les permissions qui lui ont été attribuées comme le montre l'image ci-dessous. Notons également que le propriétaire des données peut révoquer les permissions d'un

utilisateur qui a accès à ses données. Pour cela, il faut sélectionner l'utilisateur et cliquer sur « Remove member ».

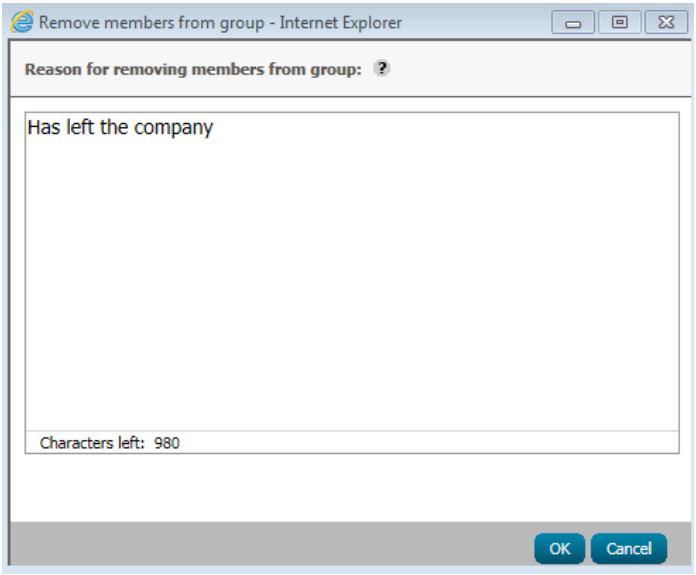
Figure 29: Droits d'accès et permissions de l'utilisateur ajouté



(Christian Djoumessi)

Ensuite, il faut entrer la raison de la révocation des permissions et valider l'action.

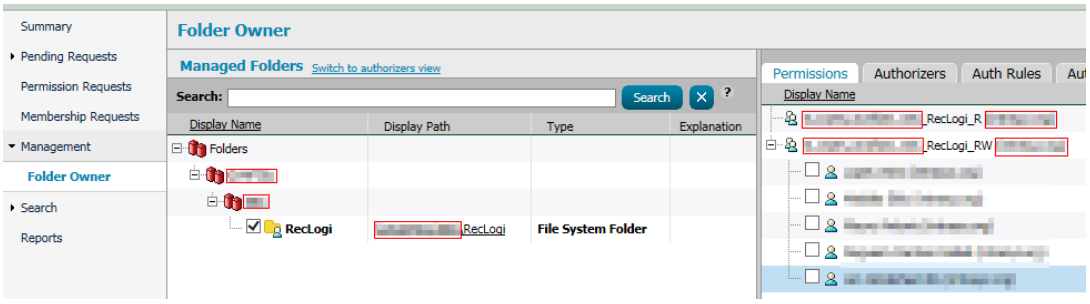
Figure 30: Révocation des droits d'accès



(Christian Djoumessi)

Comme l'illustre l'image ci-dessous, l'utilisateur n'est plus dans le groupe associé, et donc n'a plus les permissions au préalable obtenues.

Figure 31: Droits d'accès et permissions - utilisateur révoqué



(Christian Djoumessi)

Une question peut se poser, à savoir si le propriétaire des données, pour une quelconque raison le concernant, ne peut pas attribuer les droits d'accès, qui le fera ? Dans Varonis DataPrivilege, un propriétaire de données peut ajouter des délégués dit « Authorizer » par répertoire, qui sera donc capable de suivre la procédure précédemment décrite.

Dans cette situation, trois avantages s'offrent en matière de gouvernance de données contre la fuite celle-ci :

- L'application du principe de moindre privilège, car une partie des personnes identifiées dans le workflow initial est retirée
- La rapidité de l'attribution des droits d'accès, et surtout de révocation des accès, car il n'y aura pas d'attente de l'équipe IT pour appliquer la révocation, elle est directement faite par le propriétaire de données. Ce dernier cas est très sensible car dans une situation ou un collaborateur se fait licencier ou démissionne, il faut agir rapidement sur ses droits d'accès
- Tous les événements effectués sur les droits d'accès (d'attributions et révocations) sont journalisés et visibles dans la console Varonis DataPriviledge au travers d'une simple recherche. Ceci permet de fournir des informations lors des investigations ou des audits de sécurité sur les droits d'accès

6. Analyse des objectifs

6.1 Objectifs du Groupe

Le groupe est exposé à plusieurs risques internes. L'un des risques majeurs est le risque de fraude, dont le vol de données est une composante qui est particulièrement suivie. Il était attendu que le présent travail permette :

- D'améliorer le cadre de réalisation DLP au moyen d'une configuration plus nette de l'outil utilisé pour ce contrôle
- De rendre plus efficace et plus fiable la détection des anomalies à travers une meilleure gestion des règles incluant de bonnes documentations et des procédures de test
- D'optimiser la réalisation du contrôle à proprement parler, en fluidifiant la gestion des anomalies, en particulier celle qui sont qualifiées en incidents

D'autre part, le Groupe, qui est en pleine revue de son catalogue de contrôle, porte un accent particulier à la gestion des risques externes. Les technologies du Cloud présentent un enjeu particulier dans l'identification des facteurs de risques du futur. Pour cette raison il était attendu que les questions relatives à la fuite de données dans ce type d'environnement soient abordées dans le cadre de ce travail. Dans l'intérêt de l'étudiant que je suis, le Groupe a également souhaité procéder à une initiation au SIEM utilisé dans son système d'information.

Comme nous l'avons évoqué dans les sections précédentes, l'« or virtuel » que constitue les données, doit être protégé, comme toute richesse. Le premier moyen de protection étant le contrôle d'accès, ma contribution à la revue périodique de ceux-ci était très attendue. C'est dans cette optique que les actions suivantes ont été réalisées :

- Avec l'équipe en charge de la sécurité des systèmes d'information, nous avons procéder à une revue de l'utilisation de l'outil sur lequel se base l'exercice de revalidation des accès.
- La campagne de revalidation des d'accès aux applications critiques a été réalisée avec succès et une grande partie de ce contrôle se fait désormais de manière automatique.
- La campagne de revalidation des accès aux répertoires est totalement automatisée et les responsables métiers sont désormais familiarisés à cet exercice, à tel point que le Groupe envisage d'en augmenter la fréquence.

Le Groupe a exprimé sa satisfaction par rapport aux objectifs qu'elle m'avait fixés dans le cadre de ce travail de Bachelor. En dépit du fait que la mise en place de deux contrôles liés au Cloud n'a pas été effectué, tous les autres objectifs ont été largement atteints voire même dépassés.

6.2 Objectifs personnels

En ce qui me concerne, je suis très honoré d'avoir travaillé au contact direct d'une équipe de professionnels qui opèrent dans un domaine aussi sensible. Mes principaux acquis lors de cette expérience professionnelle peuvent se résumer de la manière suivante :

- J’ai découvert d’autres métiers de l’informatique (Applications, systèmes, réseau, support…) et j’ai pu me familiariser à leur quotidien. À titre d’exemple, je sais dormais la criticité et la difficulté que représente le bon fonctionnement d’un environnement informatique de production
- J’ai une bonne vision des différentes activités liées à la sécurité des systèmes d’information, car j’ai été impliqué de près ou de loin à des actions telles que : la sensibilisation aux utilisateurs, la protection des données, l’identification et l’évaluation des risques, la mise en place de mesures d’atténuation, la mise en place et la réalisation de contrôles…
- J’ai acquis une vision transverse des métiers de la banque

J’ai pu réaliser des actions pratiques liées au cours de « Gouvernance de la sécurité » que j’ai suivi en deuxième année. À ce titre je peux citer les exemples suivants : Les menaces et objectifs de sécurité, la gestion des risques, la sensibilisation…

La réalisation de ce travail de diplôme m’a donc permis de m’affirmer dans plusieurs domaines. Notamment cela a été une manière très efficace de découvrir le monde professionnel ; autant du point de vue de la découverte du fonctionnement d’une entreprise que du point de vue personnel où j’ai touché du doigt les différentes possibilités de carrière qui pourront s’ouvrir à moi.

Dans la conclusion, nous reviendront sur les aspects des objectifs de ce travail.

8. Conclusion

Ce travail de Bachelor m'a permis de pouvoir apporter ma contribution à l'équipe en charge de la cyber-sécurité du Groupe dans la gestion des risques liés à la fuite de données. J'ai pu mettre en pratique mes compétences acquises durant le stage, notamment dans les points suivants :

- Gestion de l'outil Forcepoint DLP
  - Configuration de nouvelles règles DLP
  - Optimisation des règles DLP existantes
  - Intégration du métier dans le processus de définition de nouvelles règles DLP
  - Documentation des règles DLP et proposition d'une procédure de revue de celles-ci
- Mise en place d'un contrôle pour la disponibilité et la visualisation des services DLP via le SIEM Splunk
- Revalidation des accès aux répertoires sensibles
  - Tests pour préparer la revalidation des accès
  - Configuration de l'outil Varonis DataPrivilege pour l'automatisation de la revalidation des accès
  - Suivi actif de la campagne de revalidation des accès ; du lancement à la clôture de la campagne

J'ai également pu apporter ma contribution lors de la définition du processus de réponse aux incidents en proposant des améliorations.

Sur le plan académique, ce travail m'a permis de faire le lien avec la théorie apprise durant le cours de « Gouvernance de la sécurité » et ajouter une brique de compétence technique au cours « Sécurité des réseaux ». Les différents enseignements reçus tout au long du cursus Bachelor of Science HES-SO en Informatique de Gestion, ont été des facilitateurs dans mon intégration au milieu professionnel. Ceci m'a donné plus d'assurance et de confiance pour remplir ma mission.

J'ai pu acquérir des compétences techniques et organisationnelles en matière de gestion des risques. Je suis heureux de savoir que le produit de mon travail est utilisé quotidiennement au sein de l'entreprise qui m'a permis de le réaliser. Ce stage m'a également permis d'élargir mes horizons quant aux possibilités futures de l'orientation de ma carrière.

Pour conclure, il est à noter que la technologie ne règle pas tous les problèmes, puisque certains risques peuvent ne pas être couverts. De plus, les méthodes de gestion des risques doivent s'adapter à l'évolution permanente des techniques numériques ; la technologie en elle-même ne

doit pas devenir un facteur de risques, mais un moyen de faire face aux différents enjeux rencontrés au courant de la vie.

Bibliographie

Les données de 530.000 comptes Zoom en vente sur le dark web – LeFigaro [en ligne]. [Consulté le 3 mai 2020]. Disponible à l'adresse : https://www.lefigaro.fr/secteur/high-tech/les-donnees-de-530-000-comptes-zoom-en-vente-sur-le-dark-web-20200414

Les conséquences de la fuite de données – Observatoire FIC [en ligne]. [Consulté le 3 mai 2020]. Disponible à l'adresse : https://observatoire-fic.com/les-consequences-de-la-fuite-de-donnees-perte-de-reputation-de-la-marque-et-impacts-financiers-by-seref-can-ozkaya/

Splunk Architecture: Tutorial On Forwarder, Indexer And Search Head – Edureka [en ligne]. [Consulté le 17 juin 2020]. Disponible à l'adresse : https://www.edureka.co/blog/splunk-architecture/

Data protection in a zero-perimeter world – Forcepoint [document PDF]. [Consulté le 18 juin 2020]. Disponible à l'adresse : https://www.forcepoint.com/sites/default/files/resources/brochures/brochure-dlp-en.pdf

Matrice RACI : comment définir les rôles et les responsabilités ? – Advaloris [en ligne]. [Consulté le 20 juin 2020]. Disponible à l'adresse : https://www.advaloris.ch/nos-services/intelligence-organisationnelle/bonnes-strategies-doptimisation-organisationnelle-entreprises/matrice-raci-definir-roles-responsabilites

DLP – Les fuites de données – e-xpert solutions [en ligne]. [Consulté le 27 mai 2020]. Disponible à l'adresse : https://blog.e-xpertsolutions.com/dlp-les-fuite-des-donnees/

Varonis – Saycurit [en ligne]. [Consulté le 1er mai 2020]. Disponible à l'adresse : http://www.saycurit.fr/partenaires/article/varonis

Gouvernance de l'accès aux données – Varonis [en ligne]. [Consulté le 1er mai 2020]. Disponible à l'adresse : https://www.varonis.com/fr/produits/dataprivilege/

Sécurité des entreprises : la menace vient de l'intérieur – Largeur [en ligne]. [Consulté le 28 février 2020]. Disponible à l'adresse : https://largeur.com/?p=3078

Espionnage industriel – PwC [en ligne]. [Consulté le 3 avril 2020]. Disponible à l'adresse : https://www.pwc.fr/fr/decryptages/securite/espionnage-industriel-menace-a-apprehender-avec-determination.html

L'affaire Clearstream pour les Nuls – Libération [en ligne]. [Consulté le 2 avril 2020]. Disponible à l'adresse : https://www.liberation.fr/societe/2007/07/27/l-affaire-clearstream-pour-les-nuls_11441

Les "MacronLeaks", piratage et fuite de documents du mouvement En Marche! – L'express [en ligne]. [Consulté le 2 avril 2020]. Disponible à l'adresse :

https://www.lexpress.fr/actualite/politique/elections/les-macronleaks-piratage-du-mouvement-en-marche_1905923.html

Cambridge Analytica : tout comprendre au scandale de fuite de données qui secoue Facebook – Frandroid [en ligne]. [Consulté le 20 juin 2020]. Disponible à l'adresse : https://www.frandroid.com/culture-tech/494669_cambridge-analytica-tout-comprendre-au-scandale-de-fuite-de-donnees-qui-secoue-facebook

Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook – Le Monde [en ligne]. [Consulté le 20 juin 2020]. Disponible à l'adresse : https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html

Plan de prévention et de gestion des fuites d'informations – Cairn [en ligne]. [Consulté le 28 avril 2020]. Disponible à l'adresse : https://www.cairn.info/revue-i2d-information-donnees-et-documents-2015-1-page-25.htm?contenu=article#

Comment se protéger contre les fuites de données en entreprise – ZDNet [en ligne]. [Consulté le 13 mars 2020]. Disponible à l'adresse : https://www.zdnet.fr/pratique/comment-se-proteger-contre-les-fuites-de-donnees-en-entreprise-39895015.htm

Les conséquences de la fuite de données : Perte de réputation de la marque et impacts financiers – Observatoire FIC [en ligne]. [Consulté le 14 mars 2020]. Disponible à l'adresse : https://observatoire-fic.com/les-consequences-de-la-fuite-de-donnees-perte-de-reputation-de-la-marque-et-impacts-financiers-by-seref-can-ozkaya/

Rudolf Elmer – Wikipedia : *l'encyclopédie libre* [en ligne]. Dernière modification de la page le 14 avril 2020 à 13:09. [Consulté le 29 avril 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Rudolf_Elmer

Christoph Meili – Wikipedia : *l'encyclopédie libre* [en ligne]. Dernière modification de la page le 14 avril 2020 à 20:28. [Consulté le 29 avril 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Christoph_Meili

Hervé Falciani – Wikipedia : *l'encyclopédie libre* [en ligne]. Dernière modification de la page le 21 janvier 2020 à 11:41. [Consulté le 29 avril 2020]. Disponible à l'adresse : https://fr.wikipedia.org/wiki/Herv%C3%A9_Falciani

Annexe 1 : Moyens de contrôles des risques liés au cloud

Figure 32: Moyen de contrôle des risques liés au cloud

ID	Identified risks	CIA	Applicable	Application & Interface Security	Audit Assurance & Compliance	Business Continuity Management & Operational Resilience	Change Control & Configuration Management	Data Security & Information Lifecycle Management	Datacenter Security	Encryption & Key Management	Governance and Risk Management	Identity & Access Management	Infrastructure & Virtualization Security	Mobile Security	Security Incident Management, E-Discovery, & Cloud Forensics	Threat and Vulnerability Management
1	Unauthorised access to confidential data	Confidentiality	Y		X			X	X	X	X	X		X	X	
2	Data protection flaw	Confidentiality	Y	X			X	X		X		X	X	X	X	X
3	Role misconfiguration	Confidentiality	Y		X											
4	Lack of Role based Access Control	Confidentiality	Y	X					X							
5	Unexpected/untrcontrolled data change	Intregrity	Y		X		X					X			X	
6	Backup and recovery control loss	Intregrity	Y			X					X					
7	Data ownership loss	Intregrity	Y		X						X		X			

(Mon employeur)

Annexe 2 : Échelles d’évaluation des risques du Groupe

Tableau 4: Matrice d'évaluation des risques

Catégorie	Mineur	Modéré	Majeur	Catastrophique
Quasi-certitude				
Probable				
Possible				
Rare				

(Mon employeur)

Tableau 5: Codes couleurs des niveaux de risques

Bas	
Moyen	
Haut	
Critique	

(Mon employeur)

Annexe 3 : RACI ISIR

Figure 33: Matrice RACI ISIR

Information Security Incident Response (ISIR)	ExCo	CISO	TISO	IRT	IT SD	End Users	IT Department	Business Heads	Business Continuity Officer	Crisis Coordinator	Legal & Compliance	Communication	HR	External ressources (SMEs)
PREPARATION														
Information Security Policy	A	R	C	I	I	I	I	I	C	I	I	I	I	
Information Security Incident Response Framework	A	R	C	I	I	I	I	I	I	I	I	I	I	
Crisis Management Framework	A	C	I	I	I	I	I	I	R	C	I	I	I	
IT asset inventory		I	C		C		A, R							
Business Impact Analysis		I					I	A	R					
IT architecture diagram		I	I				A, R							
Efficient online monitoring solution		A	C		I		R							
Incident response toolkit (ready to use)		A	C				R							
Incident response playbooks		A	R	C	C		R							
Incident response training		A	R	R	R		R							
End user information security awareness	A	R				I								
IDENTIFICATION														
Create ticket		A			R									
Determine context and scope of the incident		A	R	R	C	C	C	C						
Identify potentially affected systems		A	R	R	C		C							
Evaluate business impact		A						C	R	I				
Classify and prioritize incident		A	R	R										
Escalate if necessary	I	A	R	R					I	I				
Asign approriate incident handlers		A	R	I										
Coordinate communcations (internal and external) as required		A, R			C, I	I	C, I	C, I	C, I	C, I	C, I	R	C, I	
Initiate incident documentation		A	R	R										
CONTAINMENT														
Identify necessary actions that will minimize business impact		A	R	R			C	C	C					
Increase monitoring perimeter to prevent impact propagation		A	R	R			R							
Make forensic images using appropriate tools		A	R	R			R							C
Apply temporary fix to allow systems to be used in production environment		I	A	R			R							
Continue incident documentation		A	R	R										
ERADICATION														
Rebuild systems from images or implement system changes		I	A	R			R							C
Improve defenses (hardening) to prevent reinfection		I	A	R			R							C
Continue incident documentation		A	R	R										
RECOVERY														
Decide on appropriate moment to reintegrate affected systems		I	A	R			C	C	I	I				
Identify and implement necessary monitoring		A	R	R			R	C						
Perform a vulnerability assessment and penetration testing		A	R											R
Validate that system behaviour is normal		A	R				R	R	I					
LESSONS LEARNED														
Complete the incident documentation and post-mortem report		A	R	C	C	C	C	C	C	C	C	C	C	C
Convene a Lessons Learned meeting		A, R	R	I	I		I	I	I	I				
Identify areas that need improvement (to prevent future incidents)		A	R	R	C		C	C	C	C				
Agree on action plan and milestones		A	R	R	C		C	C	C	C				
Follow-up on action plan		A, R	R											

(Mon employeur)

Annexe 4 : Abréviations

Tableau 6: Liste des abréviations

Abréviation	Définition
AD	Active Directory
AuM	Asset under Management
CASB	Cloud Access Security Brocker
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COO	Chief Operating Officer
CPU	Computer Prossesing Unit
CSO	Chief Security Officer
DLP	Data Leakage/Loss Prevention
FINMA	Autorité fédérale de surveillance des marchés financiers
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infratructure as a Service
ICAP	Internet Content Adaptation Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IRT	Incidence Response Team
ISAE	International Standards for Assurance Engagements
LDAP	Lightweight Directory Access Protocol

LPD	Loi sur la Protection des Données
OCR	Optical Character Recognition
OSI	Open Systems Interconnection
RGPD	Règlement Général sur la Protection des Données
RSSI	Responsable de la Sécurité des Systèmes d'Information
SIEM	Securit Information and Event Management
SMTP	Simple Mail Transfer Protocol
SSL	Secure Socket Layer
TCP	Transport Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator

(Christian Djoumessi)