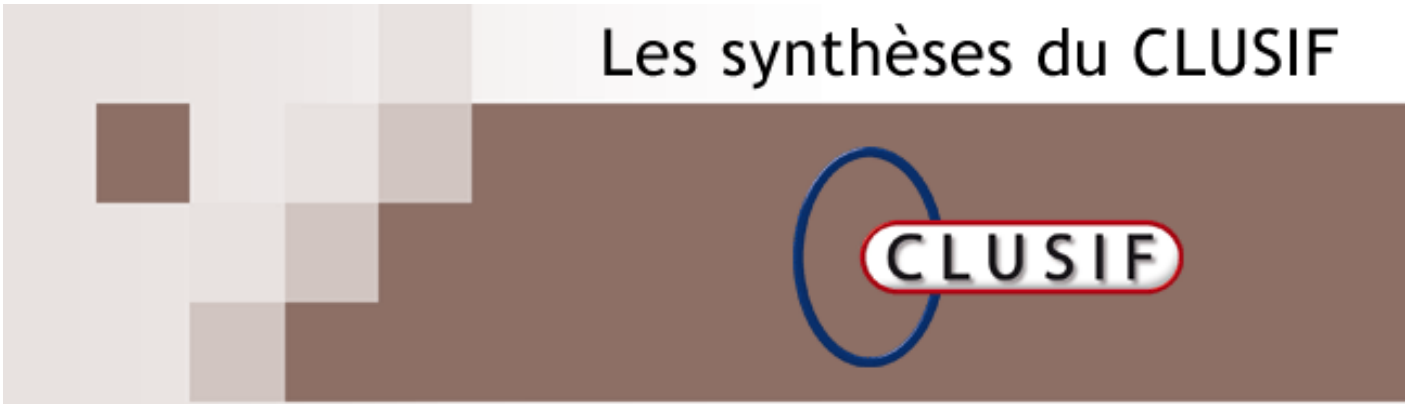

Exploiter l'information remontée par le SI

Synthèse de la conférence thématique du CLUSIF du 14 octobre 2014.

Il est un domaine de la sécurité des systèmes d'information qui s'applique tant en termes de planification que de réaction aux incidents : celui de la mesure des activités. Domaine qui consiste à regarder ce qui se passe sur le système afin d'en tirer des informations pertinentes.

Ces informations permettent de planifier la sécurité, en éditant par exemple des tableaux de bord techniques ou fonctionnels, car s'il est judicieux de mettre en place des outils et processus de sécurisation, il est aussi essentiel d'en mesurer la performance, l'efficacité et l'efficience. Ces informations permettent aussi de relever des alertes, comme le ferait un détecteur d'incendie, permettant ainsi une réaction plus rapide et appropriée à un incident de sécurité. Ces deux finalités reposent sur la capacité à collecter l'information mais aussi et surtout sur celle consistant à en extraire les informations pertinentes et exploitables.

Fort de cet état des lieux, le CLUSIF a souhaité partager son expérience sur le sujet, lors de la conférence du 14 octobre 2014. Cinq intervenants ont partagé leurs expertises et retours d'expérience : Lazaro PEJSACHOWICZ (CLUSIF), Gérard GAUDIN (Club R2GS), Jean OLIVE et Thibault CHEVILLOTTE (CGI Business Consulting), Frédéric MALMARTEL (Agence Centrale des Organismes de Sécurité Sociale - ACOSS) et Jean-Marc GREMY (CLUSIF), animateur de la table ronde.

Introduction par le CLUSIF – Lazaro PEJSACHOWICZ

Lazaro PEJSACHOWICZ introduit la conférence par un constat. L'époque où l'authentification des utilisateurs permettait d'atteindre un certain niveau de sécurité est révolue. Les entreprises et les organisations sont désormais passées d'une sécurité périmétrique à des systèmes permettant de collecter les traces laissées par le fonctionnement et l'exploitation du Système d'Information (SI).

Pour le RSSI, l'enjeu majeur va donc consister à analyser ces données ; traiter ces *journaux (log files)* stockés dans les systèmes pour permettre une surveillance, un contrôle ; et ainsi assurer une gestion des incidents de sécurité optimale.
Pour mener à bien cette gestion des incidents de sécurité, les entreprises devront notamment cartographier le SI et classifier ces évènements. On entre dans l'ère du *big data,* dans laquelle la sécurité du SI assurera les contrôles à posteriori.

L'apport clé d'un standard d'indicateurs de sécurité pour benchmarker le niveau de sécurité de son système d'information – Gérard GAUDIN (Club R2GS)

Dans un premier temps Gérard GAUDIN aborde l'état de maturité de la cyber défense et du SIEM (Security Information and Event Management).

Les solutions de SIEM apparues depuis près de dix ans répondaient bien aux attentes des entreprises en détectant tous les incidents de sécurité. Cependant, pour exploiter ces systèmes complexes, il était nécessaire de filtrer des masses de données très significatives pour obtenir au final, des résultats jugés souvent peu exploitables et décevants…

Deux axes restent donc à développer : d'une part le taux de détection des incidents, qui reste très faible (de 10 à 20%) ; et d'autre part la gestion des vulnérabilités, peu prise en compte par les équipes de production des entreprises. En effet, le guide d'hygiène informatique de l'ANSSI [1] est rarement mis en œuvre et les entreprises traitent en priorité une vision de mise en conformité réglementaire.

L'orateur met en avant la nécessité de passer d'une vision qualitative à une vision quantitative.

Cette vision consiste à benchmarker les différentes solutions et implémentations par une approche élargie, orientée indicateurs, détaillés par l'ETSI « GS ISI-001 ». [2] [3]

Gérard GAUDIN met en avant la nécessité de décloisonner la cyber sécurité et de développer une intelligence dans la détection des menaces (valeur ajoutée de la détection des incidents de sécurité).

L'objectif est de mettre l'humain au cœur de la démarche, de mobiliser le management et d'agir sur les bons leviers de motivation (notamment sur le *Pourquoi*). Cette initiative est une démarche globale de gestion de la sécurité visant à collecter et à partager l'expérience par les indicateurs de sécurité. Cette dernière est d'ores et déjà en cours de déploiement en France et Europe.

En conclusion, il s'agit d'un sujet complexe bien que la communauté SSI progresse rapidement : les instances patronales s'intéressent en effet de plus en plus aux enjeux de la cyber défense des entreprises. Enfin, ces initiatives visent à la standardisation des indicateurs tant en Europe et qu'aux États-Unis.

[1] http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
[2] http://www.etsi.org/
[3] http://www.etsi.org/deliver/etsi_gs/isi/001_099/00101/01.01.01_60/gs_isi00101v010101p.pdf

« Quand Monsieur Soc[4] rencontre Monsieur Carto[5] » - Jean OLIVE, Thibault CHEVILOTTE (CGI Business Consulting)

Dans leur intervention les deux orateurs mettent en avant une approche complémentaire.

La présentation débute par un simple constat : comment traiter efficacement les incidents de sécurité alors que l'on ne connait pas forcément son système d'information ? Les orateurs mettent en avant l'intérêt de la cartographie du SI, qui permet un traitement efficace des incidents de sécurité détectés par un SOC (Security Operation Center). Le principal enjeu consiste à exploiter au mieux les informations du SIEM, à être en mesure de détecter les anomalies et à utiliser la cartographie pour qualifier ces anomalies.

Cette cartographie permet de contextualiser les indicateurs de gestion des incidents de sécurité. En positionnant ces indicateurs dans la cartographie du SI, le RSSI sait à quel endroit se situe l'incident et visualise ainsi les composants touchés par une vulnérabilité.

On parle alors de « détection – réaction » : réagir en confinant l'incident, qualifier les impacts pour le métier, restaurer la confiance et enfin, éviter la récurrence. Cela permet d'obtenir une vision de la cohérence des mesures de sécurité issues du SOC.

On peut cartographier un SI selon deux approches. Premièrement l'approche technique : l'inventaire des composants d'infrastructures, des comptes, la liste des logiciels, etc. ; et deuxièmement l'approche fonctionnelle : via la modélisation des processus, la sécurité du SI est peu prise en compte. Ces deux visions sont complémentaires et positionnent au centre le Catalogue des applications.

Les deux intervenants proposent une méthodologie plus globale de cartographie : la Modélisation par couche. (cf. figure 1)

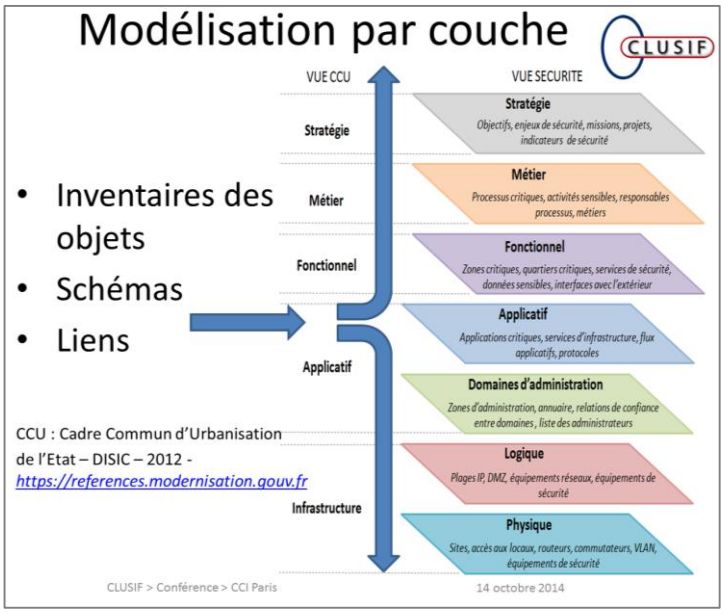

Figure 1 : Modélisation par couche

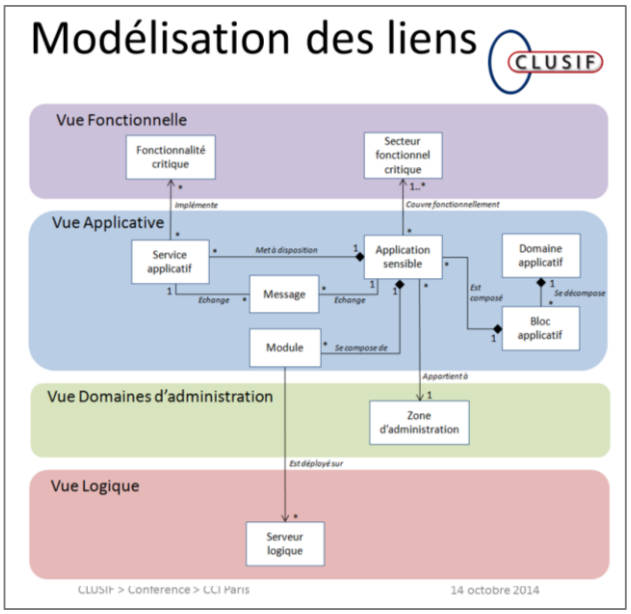

Figure 2 : Modélisation des liens

Au niveau de chaque couche, il faut inventorier les objets en intégrant des niveaux de priorité, puis modéliser les liens pour passer d'une couche à l'autre. (cf. figure 2).

Pour mettre en œuvre ce type de modélisation (urbanisation), il est conseillé d'inscrire des jalons obligatoires de remontée d'information de la cartographie dans la méthodologie des projets. Il faut démarrer par un périmètre réduit puis l'étendre dans le temps.

En conclusion, la cartographie sera utile pour positionner les sources de logs et les collecteurs, qualifier un incident de sécurité, réagir et produire des indicateurs dans leur contexte. L'objectif final est de remonter les indicateurs auprès des Directions Métiers et de la Direction Générale.

[4] Securtity Operation Center

[5] Cartographie du SI

La gestion des incidents de sécurité - L'expérience ACOSS (Agence Centrale des Organismes de Sécurité Sociale – Frédéric MALMARTEL.

Dans cet exposé, Monsieur Malmartel revient sur la mise en place de la gestion des incidents de sécurité au sein de l'ACOSS.

Le plus important est tout d'abord d'élaborer puis de suivre une procédure. Cette dernière permet de limiter l'incident au domaine initial afin qu'il reste sous contrôle et ne dégénère pas en crise. Cela permet de prévenir le risque admissible et de limiter l'incident.

Confidentialité et communication sont les deux points clés d'une telle démarche :

- la description d'un incident de sécurité est d'abord une information
- il faut se donner les moyens de maîtriser l'information dans le temps et dans l'espace.

La mise en place de procédures de marquage (tag) des incidents de sécurité et la formalisation de la procédure de qualification doivent être traitées à travers une gestion des incidents globale. L'approche consiste à démarrer de manière simple et pragmatique, en se concentrant tout d'abord sur les processus et les acteurs. L'approche ITIL (internationale) et la norme ISO 27035 ont permis de globaliser cette démarche et d'échanger avec la Direction de la Sécurité Sociale.

En conclusion, cette gestion des incidents de sécurité s'inscrit dans la démarche d'amélioration continue (conformité ISO 27001). La maîtrise des incidents de sécurité permet d'améliorer la robustesse du SI et participe activement à la mise en place d'une gestion du risque plus efficiente.

Table Ronde animée par Jean-Marc GREMY

Gérard GAUDIN (Club R2GS), Jean OLIVE et Thibault CHEVILLOTTE (CGI Business Consulting), Frédéric MALMARTEL (Agence Centrale des Organismes de Sécurité Sociale - ACOSS)

Dans la gestion des incidents de sécurité, y-a-t-il une contradiction entre la vision opérationnelle et une démarche de normalisation ? (approche normative ISO 27001 et 27035).

Frédéric MALMARTEL ne voit pas d'opposition entre la démarche de normalisation et la vision opérationnelle de la gestion des incidents de sécurité. Il faut en effet une approche « état des lieux ». S'il y a un écart avec la norme, ce dernier peut être comblé dans un second temps.

Les autres intervenants mettent en avant l'importance de la normalisation. Ces processus de gestion des incidents permettent au RSSI d'avoir une bonne vision de la DSI sous l'angle métier.

Jean OLIVE et Frédéric MALMARTEL mettent l'accent sur le pragmatisme de la cartographie du SI. Il faut mener les démarches opérationnelles et cette cartographie en parallèle. Pour commencer, l'identification des contacts est essentielle, notamment en prenant en compte les DSI au sein des métiers

Gérard GAUDIN met en avant les bénéfices d'une approche exhaustive par grand type d'incident.

Une future norme de détection des incidents des outils de SIEM est en cours d'écriture. (ISO 27044).

Faut-il des traces de sécurité dans les applications ?

Oui selon les métiers. Cette démarche, assez récente, a d'abord été implémentée au sein des SI bancaires. Il est cependant difficile d'analyser des traces dans un cadre où la diversité des contextes métiers est importante. A l'inverse, les *logs* techniques d'infrastructures sont eux beaucoup plus faciles à interpréter.

La corrélation entre les traces applicatives et les *logs* techniques est difficiles car tous deux appartiennent à des mondes distincts très différents.

Quels sont les facteurs-clés de succès pour mettre en place une gestion des incidents efficiente ?

Le rôle principal de l'équipe de gestion des incidents est d'identifier les bons interlocuteurs (les « sachants »), de mobiliser les bonnes personnes afin de résoudre les incidents tant au niveau infrastructure qu'au niveau applicatif, et de faire le lien entre les logs d'infrastructure et les traces applicatives.

Il faut une meilleure relation entre l'amont de la SSI, la gouvernance, et le niveau opérationnel des SOC. Il est préconisé d'utiliser des classifications de risque identiques entre les analyses de risques et les procédures de gestion des incidents de sécurité des CERT et des SOC.