Retour d’expérience sur la mise en place d’un Centre Opérationnel de Sécurité

Vincent Ribaillier
Centre opérationnel de sécurité des systèmes d’information ministériels (COSSIM)
Direction du numérique pour l’éducation
Ministère de l’Éducation nationale et de la Jeunesse
61-65 rue Dutot
75357 Paris Cedex 15

Résumé

Le ministère de l’Éducation nationale et de la Jeunesse (MENJ) et le ministère de l’Enseignement supérieur, de la Recherche et de l’Innovation (MESRI) se sont dotés en 2019 d’un centre opérationnel de sécurité. Le Centre Opérationnel de Sécurité des Systèmes d’Information Ministériels (COSSIM) intervient sur des missions dites synchrones (détection et réaction immédiate) et asynchrones (analyse, qualification, mesures techniques et retours d’expérience).

Cet article présente un retour d’expérience sur le démarrage de cette nouvelle entité ainsi que les différentes phases qui ont été nécessaires pour sa construction et détaille les choix effectués pour établir des interactions solides entre le centre opérationnel et les différentes équipes sécurité de l’organisation, dans un souci d’optimisation des capacités de réaction aux évènements de sécurité.

Le rôle principal du COSSIM vis-à-vis des établissements d’enseignement et de recherche est de les assister pour la gestion de leurs incidents. Cette assistance, complémentaire à celle proposée par le CERT RENATER, est orientée qualification et aide à la remédiation. Elle s’articule autour d’un service Web de déclaration et de suivi des incidents qui permettra à la communauté des RSSI d’entrer en relation avec les experts en cyberdéfense du COSSIM.

Mots-clefs

COS, SOC, MENJ, MESRI, RSSI, SSI, Gestion des incidents

1 Introduction

Les deux dernières décennies ont été marquées par de nombreux incidents de sécurité sur les systèmes d'information. Désormais, plus aucune organisation ne peut envisager de négliger la sécurité de son système d'information. La SSI (Sécurité des Systèmes d'Information) est devenue un enjeu fondamental. Si elle n'est pas parfaitement maîtrisée, les conséquences pour les organisations et les personnes peuvent être néfastes : atteinte à l'image, impacts juridiques et financiers, impact sur le fonctionnement.

Face à cette prise de conscience et un paysage sécuritaire renforcé, les « *hackers* » accroissent leurs actions offensives. Ils n'ont jamais autant redoublé d'imagination pour développer des stratégies d'attaques et s'introduire dans les ruches que sont les systèmes d'information afin d'y butiner les données, nouvelle matière précieuse des temps modernes sur laquelle repose le savoir-faire des organisations. Aucune de leurs méthodes d'attaques ne peut être ignorée par les équipes en charge de la SSI.

La mise en place d'une stratégie de défense du système d'information (SI) implique de nombreux acteurs au sein de l'organisation. Le RSSI (Responsable de la Sécurité des Systèmes d'Information) se voit confier la tâche d'organiser la SSI. Pour être efficace, la SSI doit être également gérée du point de vue opérationnel. Le centre opérationnel de sécurité souvent désigné SOC (*Security Operational Center*), afin de ne pas le confondre avec le COS (comité opérationnel de la sécurité), réunit les experts en cyberdéfense, véritables chevaliers de l'ère numérique chargés de la protection du SI.

La mission principale du SOC ne se limite pas à la mise en place des systèmes de détection. Une gestion efficace des incidents de sécurité doit être mise en œuvre de façon à ce que le SOC puisse apporter un soutien aux entités impactées. Il doit également être fortement impliqué dans le processus de sensibilisation et de formation à la SSI.

Le ministère de l'Éducation nationale et de la Jeunesse (MENJ) et le ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation (MESRI) se sont dotés en 2019 d'un SOC. Cet article présente un retour d'expérience sur la création du Centre Opérationnel de Sécurité des Systèmes d'Information ministériels (COSSIM).

La première partie du présent article détaille la méthodologie utilisée pour définir et mettre en place l'organisation. La seconde partie présente les différents projets initiés pour outiller le COSSIM.

2 Définition et mise en place de l'organisation

Le SOC ne peut pas être perçu comme un simple instrument de détection. Il doit être conçu comme une entité à part entière s'intégrant dans l'écosystème complexe dans lequel l'organisation évolue. La démarche de construction du COSSIM a démarré par une phase de modélisation de son fonctionnement dans le contexte MENJ/MESRI de façon à définir précisément ses fonctions et interactions. La phase suivante a consisté à définir les différents niveaux de support associés à la gestion des incidents en s'inspirant des référentiels existants.

2.1 Fonctions d'un SOC

Le SOC est un dispositif indispensable pour assurer le maintien en condition de sécurité du SI. Ses fonctions principales sont la détection des attaques, la gestion et l'analyse des incidents. Le SOC est également impliqué dans les processus de formation et de sensibilisation.

2.1.1 Détection des attaques

La mise en place d'une détection opérationnelle des attaques nécessite une très bonne connaissance du système d'information de l'organisation. Il est dans l'intérêt du SOC d'établir des liens privilégiés avec les équipes opérationnelles de son périmètre de détection. Le COSSIM a pu notamment tisser ces liens en participant aux différents comités opérationnels de sécurité du périmètre MENJ, ce qui lui a permis d'être moteur dans les projets de déploiement des systèmes de détection.

2.1.2 Gestion des incidents

Si la gestion des incidents n'est pas bien formalisée, chaque nouvel incident aura de grandes chances d'être anxiogène pour les équipes de l'organisation. Il est essentiel que l'organisation soit préparée à les gérer. Lorsqu'un incident est détecté, le SOC est ainsi en capacité de déployer rapidement une logistique permettant de porter assistance à l'entité impactée afin de l'aider, d'une part à contenir le sinistre, et d'autre part à définir le plan de remédiation approprié. Il est également préparé à communiquer de façon efficace avec ses nombreux interlocuteurs : RSSI, instances de pilotage, CERT (Computer Emergency Response Team ou encore centres d'alerte et de réaction aux attaques informatiques), Délégués à la protection des Données, autorités, équipes opérationnelles, utilisateurs, etc. La mise en place d'une gestion des incidents est facilitée si le SOC dispose d'un outil permettant de déclarer rapidement les incidents et de mettre en relation les différents acteurs impliqués.

2.1.3 Analyse

Le SOC est chargé d'analyser les incidents. Il instaure une méthodologie d'investigation numérique et veille à ce qu'elle soit bien maîtrisée par ses experts. Une investigation numérique débute par une phase de collecte d'information (images disques, images mémoire, traces systèmes, etc.). Il s'ensuit une phase de qualification qui consiste à rechercher les indicateurs de compromission, à déterminer la cause de l'incident, le mode opératoire de l'attaque, les vulnérabilités exploitées et l'étendue de la compromission. Le SOC joue enfin un rôle important dans la phase de remédiation, son

rôle est de proposer des mesures permettant de réduire l'exposition aux risques à un niveau acceptable.

2.1.4 Restitution

Une partie importante de l'activité du SOC consiste à restituer les informations relatives aux incidents. Cela se concrétise notamment par la production de comptes rendus détaillés d'analyse et la fourniture d'indicateurs synthétisant les impacts des incidents sur les différents périmètres du système d'information. Les incidents peuvent être par exemple répertoriés en fonction de leurs typologies et de leurs niveaux de gravité. Les indicateurs sont particulièrement utiles pour identifier les périmètres sur lesquels des investissements sont requis pour améliorer le niveau de sécurité.

L'organisation a également intérêt à mettre en avant le plus possible son SOC dans les activités de communication et de sensibilisation. Chaque incident vécu est une opportunité de consolider les compétences des experts en cyberdéfense et d'améliorer le processus de gestion des incidents. L'analyse d'un épisode de gestion d'incident permet d'identifier les actions entreprises qui ont fonctionné ainsi que celles qui sont perfectibles. Il est essentiel d'apprendre de ses erreurs. Cela peut consister par exemple à réviser les fiches réflexes ou à améliorer certains processus.

La présentation de retours d'expérience sur des incidents vécus présente l'avantage de mettre en situation l'auditoire et de lui faire prendre conscience de la nécessité d'accroître sa vigilance dans la conduite des différents projets impactant le SI. Le volet SSI d'un projet doit être piloté pendant toute sa durée de vie et non pas uniquement au moment de la mise en production. Les exploitants des systèmes d'information constituent une cible prioritaire dans la démarche de sensibilisation. Il est important de s'assurer qu'ils ont bien pris conscience de la nécessité de maintenir en condition de sécurité les systèmes d'information. Les incidents ont souvent pour cause une négligence. En pensant économiser quelques heures de travail, l'équipe à l'origine de l'incident peut mettre toute une communauté en émoi et générer un surcoût de travail conséquent pour l'ensemble de l'organisation, les impacts pouvant être très significatifs pour l'organisation (opérationnel : suspension du service aux usagers pendant plusieurs mois, juridique, financier, atteinte à l'image, etc.).

Il est nécessaire d'orienter le discours de sensibilisation en fonction de l'auditoire. Les retours d'expérience du SOC s'adressent également aux utilisateurs finaux qui apprécieront de découvrir les coulisses de la cybersécurité et de mieux comprendre les enjeux pour leur organisation.

2.2 Identification des interactions

2.2.1 Experts SSI

Les spécialistes en SSI interagissent fréquemment avec le SOC qui leur restitue sa compréhension de l'incident et leur propose des actions de remédiation. Ces actions peuvent pour les cas les plus critiques nécessiter l'arrêt d'un service ; il reviendra au RSSI de les valider et de les relayer aux équipes métiers chargés de la maîtrise d'ouvrage.

Le SOC est chargé de fédérer les équipes opérationnelles impliquées dans la sécurisation du SI. Il participe aux différents comités opérationnels de sécurité instaurés

dans l'organisation. Cela lui permet de bien intégrer les problématiques SSI vécues quotidiennement par les équipes, d'établir des liens de confiance qui s'avéreront être très précieux lors des épisodes de gestion de crise. Le SOC éclaire les équipes sur l'état de la menace et les conseille dans la mise en œuvre des mesures de sécurité. Ces nombreux échanges facilitent le processus de formalisation et de gestion des incidents.

Le SOC collabore avec les centres d'alerte et de réaction aux attaques informatiques que sont les CERT ou CSIRT (*Computer Security Incident Response Team*). Le SOC peut déléguer partiellement ou entièrement les fonctions d'alertes et de réaction aux attaques à un CERT ou au contraire les assurer pleinement. Dans tous les cas, il a intérêt à rejoindre des groupes de travail regroupant les différents CERT pour échanger des informations sur les techniques d'attaques, les indicateurs de compromissions (IOC) ou les bonnes pratiques.

2.2.2 Instances de pilotage

Le SOC fournit régulièrement aux instances de pilotage des indicateurs sur les incidents en cours et les niveaux d'exposition aux risques de l'organisation. À chaque nouvel épisode de gestion d'incident, il leur restitue l'état d'avancement des analyses et des actions de remédiation entreprises. En étant bien informées du niveau de maturité du SOC et de son offre de service, les instances de pilotage pourront plus facilement le mettre en avant dans la démarche de communication instaurée dans l'organisation. Cela renforcera les liens de confiance établis entre l'organisation et les différents partenaires.

2.2.3 Autorités

Le SOC est un interlocuteur privilégié des autorités impliquées dans la gestion des risques et des incidents. Le COSSIM est chargé de fournir les comptes rendus d'incidents à l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Il séquestre les différents éléments issus des analyses afin de les remettre aux autorités judiciaires compétentes le cas échéant.

2.2.4 Utilisateurs

L'analyse de certaines attaques nécessite de comprendre les actions effectuées par les utilisateurs du système d'information. Dans le cas d'une campagne d'hameçonnage, le SOC peut par exemple être amené à contacter un utilisateur pour comprendre les actions effectuées par ce dernier. Ces moments d'échanges sont aussi une opportunité pour le SOC de diffuser des bonnes pratiques aux utilisateurs.

2.3 Définition des niveaux de supports

L'une des priorités pour l'établissement du COSSIM a été de définir les différents niveaux de support. D'une organisation à l'autre les niveaux de support proposés par les SOC n'ont pas nécessairement la même signification. Le SOC peut s'appuyer sur l'expertise de partenaires pour assurer certaines de ses missions en recourant par exemple aux services d'un CERT. L'organisation mise en place dans le projet d'établissement du COSSIM intègre trois niveaux de support.

2.3.1 Support de niveau 1 : détection et réception des signalements

Le premier niveau de support est chargé de la détection et du recensement des différents signalements d'incidents. Cette mission est assurée en grande partie par le CERT RENATER qui est outillé pour surveiller les flux échangés sur le réseau qu'il opère et

qui interconnecte 1300 sites de la communauté Éducation – Recherche. Le COSSIM est également en capacité de détecter les incidents de sécurité sur les périmètres internes du MENJ les plus sensibles.

Dans ce contexte, le CERT RENATER a pour mission de relayer les alertes et signalements aux différentes entités du périmètre MENJ/MESRI. Les signalements qu'il réceptionne proviennent de CERTs tels que le CERT-FR opéré par l'ANSSI mais également de leveurs d'alertes, chasseurs de bogues ou des utilisateurs des systèmes d'information.

L'organisation qui a été définie et qui est actuellement en cours de déploiement s'articule autour d'un outil de signalement et de gestion des incidents dont les fonctionnalités sont présentées en deuxième partie de cet article. Cet outil permettra aux différents RSSI de la communauté de suivre les incidents impactant leurs périmètres et de solliciter une assistance du COSSIM. Il sera accompagné de consignes claires qui détailleront les précautions à prendre avant de transmettre des documents sensibles (chiffrement).

2.3.2 Support de niveau 2 : analyse et qualification

Le deuxième niveau de support de ce dispositif, assuré par l'équipe du COSSIM, est chargé de l'analyse des incidents les plus significatifs.

Le mode de support varie en fonction du contexte. Les principaux paramètres pris en compte pour le dimensionnement de la prestation d'analyse et de réponse à incident sont, d'une part la gravité de l'incident estimée pour l'organisation et pour le ministère, et d'autre part les ressources humaines en expertise SSI disponibles dans l'entité impactée et dans l'équipe COSSIM. Ainsi, selon le contexte, le COSSIM est mandaté pour conduire l'intégralité de l'analyse, ou pour assister l'entité dans la démarche d'analyse en lui fournissant les conseils et la documentation nécessaire.

Dans les cas d'incidents de gravité importante impliquant un processus d'analyse et de qualification très coûteux en ressources humaines, tels que par exemple une intrusion suivie d'une propagation latérale sur de nombreux éléments sensibles du système d'information, le COSSIM peut être accompagné dans sa démarche par l'ANSSI. Il peut également recourir aux services de prestataires spécialisés en réponse aux incidents.

2.3.3 Support de niveau 3 : aide à la remédiation

Le troisième niveau de support, également assuré par le COSSIM, consiste à assister l'entité impactée dans la remédiation de l'incident. Une stratégie de remédiation est proposée au RSSI de l'entité et est révisée au fur et à mesure de l'avancement de l'analyse des informations collectées.

Le COSSIM intervient également pour vérifier que les systèmes impactés ont été correctement assainis et pour s'assurer que les mesures retenues sont suffisantes pour ne pas exposer à nouveau les ressources aux mêmes risques. Le COSSIM est outillé pour effectuer des scans de vulnérabilités sur les systèmes d'information afin de vérifier la robustesse des services. Pour les incidents impactant les entités relevant du périmètre MENJ, le COSSIM peut solliciter l'aide du pôle national de compétences en sécurité des systèmes d'information du MENJ pour qu'un audit complet soit réalisé avant la remise en production du service.

2.4 S’inspirer des référentiels

Les différents référentiels liés à la gestion des incidents ont été très utiles dans la démarche de construction du COSSIM. Les principaux référentiels qui ont servi de référence sont résumés dans cette section.

2.4.1 RFC 2350

La RFC 2350 (*Expections for Computer Security Incident Response*) [1] s’adresse aux équipes chargées de répondre aux incidents de sécurité (*Incident Response Team* ou *IRT*) et leur propose un cadre pour se présenter aux communautés qu’elles servent. Le formalisme présenté permet de décrire l’équipe, ses missions, son périmètre d’intervention, la procédure à suivre pour entrer en contact avec elle. Le groupe InterCERT-FR piloté par l’ANSSI et qui réunit un ensemble d’organismes français ayant des activités d’IRT sur le territoire français référence l’ensemble des RFC 2350 de ses membres.

2.4.2 Le modèle SIM3

Le modèle SIM3 (*Security Incident Management Maturity Model*) [2] mis en avant par L’Open CSIRT Foundation et le programme *Trusted Introducer* du TF-CSIRT propose d’évaluer le niveau de maturité de la gestion des incidents de sécurité mis en place dans une organisation. Une quarantaine de critères d’évaluation sont répartis en quatre grandes thématiques : paramètres organisationnels, gestion des ressources humaines, outillages et processus. La maturité de chacun des paramètres est appréciée sur une échelle allant de 0 à 4. Ce modèle permet ainsi de confronter le niveau de maturité réel de l’organisation au niveau de référence visé.

2.4.3 Le modèle d’évaluation proposé par l’ENISA

L’ENISA propose une méthode *ENISA CSIRT assesment model* [3] basée sur le modèle SIM3 et intégrant les obligations de la directive européenne NIS. Chacun des paramètres est évalué selon une échelle à trois niveaux : *basic, inermediate, advanced.* Cette méthode est accompagnée du guide *ENISA Maturity Evaluation Methodology* [4] *for CSIRTs* présentant une méthode permettant à l’équipe CSIRT de s’autoévaluer ainsi qu’une méthode permettant d’instaurer un processus d’évaluation des pairs au sein d’un groupe de CSIRTs (*peer review workshop*).

2.4.4 PDIS

Le référentiel PDIS [5] publié par l’ANSSI est un référentiel d’exigences applicables pour les prestataires spécialisés en détection des incidents de sécurité. Ce référentiel a été élaboré dans le but de qualifier les prestataires chargés de la détection des incidents dans des secteurs d’importance vitale soumis au respect de la réglementation de la loi de programmation militaire. Il peut être également utilisé en tant que référentiel de bonnes pratiques et s’avère à ce titre très utile dans la démarche de construction du SOC qui pourra identifier les exigences prioritaires à respecter dans son contexte.

2.4.5 PRIS

Le référentiel PRIS [6] également publié par l’ANSSI, détaille les exigences relatives au déroulement d’une prestation de réponse aux incidents de sécurité. Il se focalise sur les prestations de recherche d’indicateurs de compromission et d’investigations numériques. Les exigences couvrent également les processus relatifs à l’organisation et

la gouvernance (charte éthique, gestion des ressources et des compétences) ainsi qu'à la protection de l'information. La phase d'exécution de la prestation mérite une attention particulière car elle décrit le processus itératif consistant à réviser la posture et les mesures de remédiation en fonction des analyses effectuées sur les informations collectées. Les différentes étapes de cette phase sont résumées sur le schéma ci-dessous :

Figure 1 - Phase d'exécution d'une prestation de réponse à incident

2.4.6 ISO/IEC 27035

Le référentiel ISO/IEC 27035 [7] propose un référentiel de gestion des incidents de sécurité au sein d'une organisation reposant sur le principe d'amélioration continue.

3 Mise en place de l'outillage

La phase d'outillage est une étape importante dans le processus de construction du COSSIM. Elle a pour objet l'identification et le déploiement des outils lui permettant d'assurer ses différentes missions. Ce processus se veut très structurant.

3.1 Détection

3.1.1 SIEM

Le SIEM (*security information and event management*) est l'outil central permettant d'assurer la fonction de détection au sein du SOC. Il assure la collecte des différents évènements de sécurité (journaux systèmes des équipements du SI, journaux applicatifs, flux réseaux) et dispose d'un moteur de corrélation capable d'identifier en temps réel les schémas d'attaque et de générer des alertes. Il est également doté d'une fonctionnalité d'archivage à valeur probante. Les différents évènements collectés peuvent ainsi être conservés de façon sécurisée au format brut et remis aux autorités le cas échéant. Lorsqu'un incident est détecté ou suspecté, les experts en cyberdéfense du SOC utilisent les fonctionnalités de fouilles de données intégrées dans le SIEM pour conduire leurs investigations. Selon les périmètres, une offre fonctionnelle de puits de logs associé à des modules de recherche de type SIEM sera disponible et interconnectée au moteur de recherche central pour assistance de ces périmètres.

3.1.2 Scanner de vulnérabilités

Le déploiement d'une solution de scanner de vulnérabilités a été également jugée prioritaire dans l'établissement du COSSIM. Cet outil est un élément essentiel dans le processus de maintien en condition de sécurité du système d'information. Il permet non seulement de déceler de façon proactive les vulnérabilités référencées dans la base CVE (*Common Vulnerabilities and Exposures*) mais également d'identifier les défauts de configuration. La vocation première de ce scanner est de sonder les back-offices avec une capacité d'introspection modulable pouvant rechercher les vulnérabilités profondes au sein des SI. Il pourra être mis à contribution sur les fronteaux le cas échéant.

3.1.3 Élaboration d'une stratégie de SOC

Le déploiement du SIEM et du scanner de vulnérabilités est une étape déterminante dans le processus de construction du COSSIM. Ce projet a pour objectif de définir une stratégie basée sur la définition d'un modèle de centre opérationnel de sécurité de référence permettant, d'une part de garantir une autonomie aux équipes opérationnelles, et d'autre part de positionner le COSSIM comme l'organe de contrôle central. L'élaboration et le déploiement du modèle de référence sont en cours sur la plate-forme nationale d'hébergement mutualisé (PHM) du MENJ identifiée comme prioritaire dans ce projet et qui dispose déjà d'un SOC. D'autres périmètres ont d'ores et déjà été sélectionnés pour implémenter ce modèle.

L'organisation mise en place dans ce projet confère au COSSIM un rôle central et fédérateur. Chaque SOC outillé est autonome pour superviser la sécurité de son périmètre. La configuration définie pour le SIEM et le scanner de vulnérabilités permettront au COSSIM d'avoir une visibilité complète sur les différents évènements de sécurité. Le COSSIM assurera un rôle moteur pour la définition et la diffusion des

règles de détection. De par son positionnement central, le COSSIM sera ainsi un maillon essentiel dans le dispositif de supervision mis en place. Il attachera une importance particulière à élaborer des règles de détection de scénarios d'attaques impliquant les différents périmètres du projet. Il sera également en capacité de lancer des investigations sur chacun des domaines sans impacter les performances des moteurs de corrélations temps-réel. Ses liens privilégiés avec les différents CERTs lui permettront d'être informé des nouvelles techniques d'attaques et des indicateurs de compromissions associés (IOC). Il pourra injecter dans le SIEM les IOC et lancer des investigations sur les périmètres fédérés afin de vérifier que ces derniers n'ont pas été impactés.

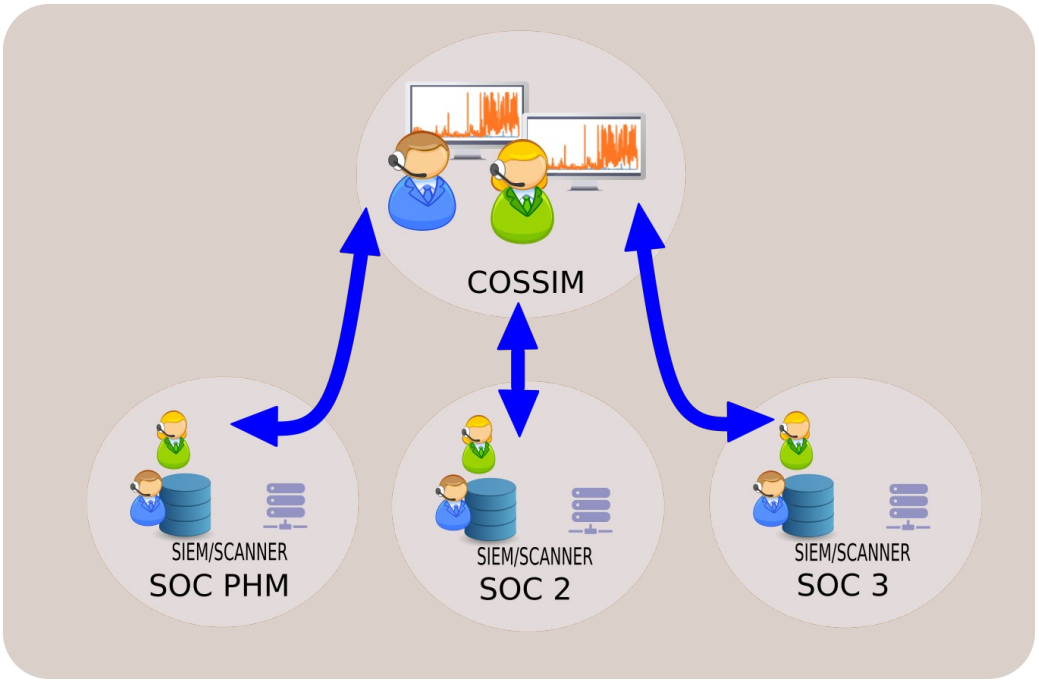

Figure 2 – Interactions du COSSIM et des SOC

La mise en place de cet outillage fait également l'objet d'une démarche d'analyse de risque te type EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) coordonnée par le pôle national de compétences en sécurité des systèmes d'information du MENJ. Cette démarche s'appuie sur les domaines fonctionnels liés aux métiers du ministère et sur l'expérience des acteurs de la chaîne SSI, les études de risques et homologations de sécurité existantes et vise à établir les mesures de sécurité associées au SOC en adéquation avec les exigences réglementaires. La démarche débouchera sur l'élaboration d'un catalogue de services. Les exploitants pourront sélectionner le niveau sécurité le plus approprié pour protéger les services et applications sous leurs responsabilités.

3.2 Gestion des incidents

Le projet de mise en place de l'outillage associé à la déclaration et au suivi des incidents de sécurité a été réalisé en étroite collaboration avec le CERT RENATER. Il a débuté par une phase de modélisation des processus de signalement et de suivi des incidents qui a débouché sur la formalisation d'un scénario pour chaque source de signalement : RSSI d'une entité du périmètre MENJ/MESRI, CERT, COSSIM, signalement externe.

La phase suivante d'établissement des spécifications de l'outillage a été conduite avec l'objectif de faciliter les interactions entre les différents acteurs impliqués dans la gestion des incidents et de permettre, d'une part au COSSIM d'avoir une visibilité complète sur les différents incidents de sécurité significatifs, et d'autre part aux instances de pilotage d'avoir facilement accès aux indicateurs liés aux incidents de sécurité. L'outil permet aux RSSI des unités impactées par un incident de sécurité de solliciter l'assistance du COSSIM qui sera ainsi en mesure de les aider sur les phases de qualification et de remédiation.

La phase d'établissement des spécifications a également eu pour objet la définition d'une classification des différentes typologies d'incidents. Cette classification a été organisée avec deux niveaux de profondeur : le premier niveau correspond à une classification générale exploitable par les instances de pilotage, le deuxième niveau est une classification technique compréhensible des experts en cyberdéfense.

Dans un souci de fournir des indicateurs aux instances de pilotage, des échelles de gravité et d'impact ont également été définies. Avant de clôturer un incident de sécurité, les RSSI seront ainsi invités à renseigner la gravité ainsi que les impacts sur leurs organisations. Cinq échelles d'impact sont proposées :

- coût financier
- coût en jours-hommes
- impact juridique
- impact sur le fonctionnement
- atteinte à l'image

Les RSSI préciseront également si les données personnelles ou les données relevant du dispositif de Protection du Potentiel Scientifique et Technique de la nation (PPST) sont impactées. Les instances de pilotage seront ainsi en mesure d'évaluer précisément les conséquences d'un incident de sécurité pour l'organisation, ce qui permettra d'une part d'accentuer les efforts de prévention, et d'autre part de mieux identifier les besoins financiers et en ressources humaines nécessaires pour réduire le niveau d'exposition aux risques.

Les données collectées dans le cadre de la gestion d'un incident étant par définition très sensibles, toutes les précautions nécessaires ont été prises pour garantir leur sécurité. Cela a consisté à héberger le service dans un environnement dédié, à configurer des mécanismes d'authentification et de chiffrement. Toutes les pièces jointes déposées sur le serveur par le RSSI sont automatiquement chiffrées et déchiffrables uniquement par les membres du COSSIM. Les RSSI sont par ailleurs invités à chiffrer les documents les

plus sensibles (journaux de connexion, dépôts de plaintes, etc.) à l'aide d'un outil qualifié par l'ANSSI.

3.3 Analyse

Afin de pouvoir réaliser les investigations numériques, le COSSIM s'est équipé d'outils spécifiques.

3.3.1 Analyses en ligne

Les stations d'analyse en ligne disposent des derniers outils logiciels permettant de scanner les systèmes sur lesquels une compromission est suspectée ou avérée. L'environnement de référence est la distribution LINUX KALI [8] qui inclut une collection d'outils en sources ouvertes. Certains outils propriétaires font également partie de la boîte à outil des experts en cyberdéfense de l'équipe.

3.3.2 Analyses inforensiques

L'analyse des différents éléments collectés tels que les images disque, images mémoire, journaux d'évènements, alertes, traces système, traces réseau, traces applicatives est réalisée à l'aide d'outils matériels et logiciels spécialisés. Les données collectées sont centralisées sur des stations dédiées aux analyses inforensiques et dotées d'une puissance de calcul et d'une capacité de stockage significative. Les stations ne sont pas connectées sur le réseau et sont chiffrées à l'aide d'algorithmes de chiffrement robustes. Les analyses inforensiques sont réalisées à l'aide de bloqueurs en écritures qui permettent d'effectuer des copies intégrales des disques sans altérer l'intégrité des données qu'ils contiennent. Les éléments collectés sont conservés dans un coffre-fort.

Figure 3 : Analyse forensique sur un disque réalisée à l'aide d'un bloqueur en écriture

Figure 4 : Station d'analyse forensique

3.4 Restitution

Le COSSIM maintient une collection de retours d'expérience et de scénarios d'attaques types qui peuvent être rejoués lors des séances de sensibilisation à la SSI. Ils sont utilisés également pour former et maintenir des compétences des experts en cyberdéfense. Les scénarios d'attaques sont élaborés à partir d'incidents vécus. Les

environnements des machines impactées sont reproduits et anonymisés dans des machines virtuelles.

Conclusion

En se dotant d'un centre opérationnel de sécurité, le MENJ et le MESRI affichent leur volonté de renforcer le dispositif de sécurité de l'ensemble du périmètre Éducation – Recherche. Le COSSIM est positionné dans cet écosystème complexe comme un élément central et fédérateur. Sa construction a nécessité une phase de modélisation et de formalisation des processus. Une attention particulière a été apportée à la définition de ses missions et de ses interactions avec les différents acteurs SSI impliqués dans ce dispositif. Les bonnes pratiques et principes mis en avant dans les référentiels de gestion d'incidents ont été respectés. Un processus de support à trois niveaux est instauré : détection/signalement, qualification et remédiation.

Cette étape de formalisation est accompagnée d'une phase d'outillage fortement structurante pour le centre. Le déploiement actuellement en cours d'un SIEM et d'un SCANNER (à vocation interne et externe) sur un large périmètre considéré comme prioritaire sera élargi à d'autres périmètres. Le processus de modélisation a également permis de concevoir un outil de déclaration et de suivi des incidents qui sera prochainement ouvert à la communauté des RSSI du périmètre MENJ/MESRI.

ANNEXE 1 : Liste des acronymes

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CERT	Computer Emergency Response Team (Centres d'alerte et de réaction aux attaques informatiques)
CSIRT	Computer Security Incident Response Team
CVE	Common Vulnerabilities and Exposures
COS	Comité Opérationnel de la Sécurité
COSSIM	Centre Opérationnel de Sécurité des Systèmes d'Information Ministériels
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
IOC	Indicators Of Compromise (Indicateurs de Compromission)
IRT	Incident Response Team ou IRT
MENJ	Ministère de l'Éducation Nationale et de la Jeunesse
MESRI	Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation
NIS	Network and Information Security
PHM	Plate-forme nationale d'Hébergement Mutualisé du MENJ
PPST	Protection du Potentiel Scientifique et Technique de la nation
RSSI	Responsable de la sécurité des systèmes d'information
SIEM	Security Information and Event Management
SIM3	Security Incident Management Maturity Model
SSI	Sécurité des Systèmes d'Information
SOC	Security Operations Center

Bibliographie

[1] RFC 2350, Expectations for Computer Security Incident Response, 1998 ; https://www.ietf.org/rfc/rfc2350.txt

[2] Don Stikvoort, SIM3 :Security IncidentManagement Maturity Model, 30 mars 2015, https://ocfweb.files.wordpress.com/2019/09/sim3-mkxviiic.pdf

[3] ENISA, ENISA CSIRT maturity assessment model, 30 avril 2019 https://www.enisa.europa.eu/publications/study-on-csirt-maturity

[4] ENISA, ENISA Maturity Evaluation Methodology for CSIRTs, 9 avril 2019, https://www.enisa.europa.eu/publications/study-on-csirt-maturity-evaluation-process

[5] ANSSI, Prestataires de détection des incidents de sécurité - Référentiel d'exigences, Version 2.0 d u 21 décembre 2017, https://www.ssi.gouv.fr/uploads/2014/12/pdis_referentiel_v2.0.pdf

[6] ANSSI, Prestataires de réponse aux incidents de sécurité - Référentiel d'exigences, Version 2.0 du 2 août 2017, https://www.ssi.gouv.fr/uploads/2014/12/pris_referentiel_v2.0.pdf

[7] ISO/IEC 27035-1:2016, Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information, novembre 2016, https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27035:-2:ed-1:v1:en

[8] Distribution LINUX KALI, https://www.kali.org