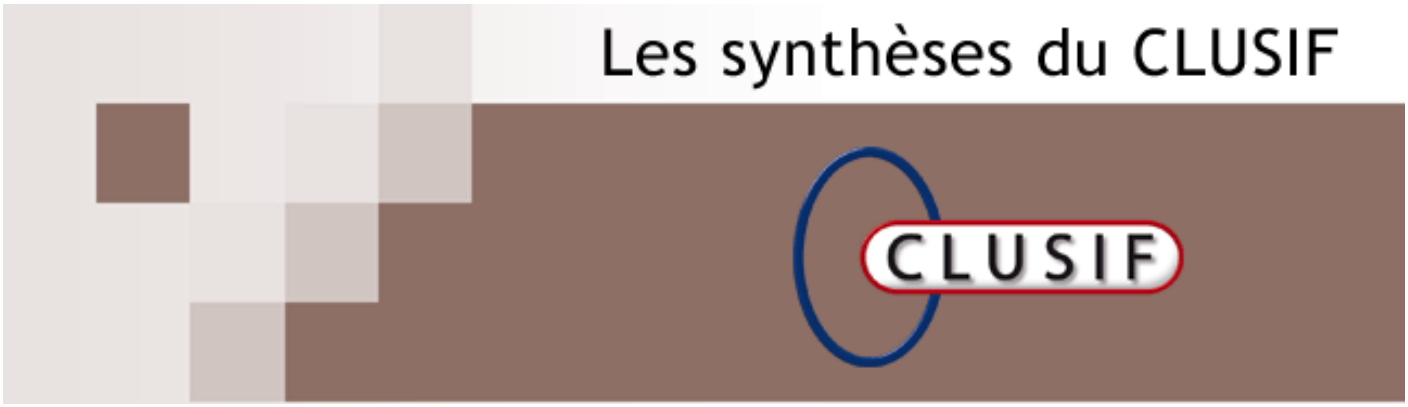

Un SOC adapté à chacun - *Synthèse de la conférence thématique du CLUSIF du 7 décembre 2016.*

La mise en place d'un SOC (Security Operation Center) est un projet central en matière de sécurité des systèmes d'information. Il comporte de nombreux obstacles et mérite un investissement approfondi de très nombreuses parties prenantes d'une organisation qui fait le choix de le déployer. C'est pour répondre à ces problématiques variées que le groupe de travail SOC du CLUSIF a produit un document de référence permettant d'anticiper et de réussir ce type de projet.

Le choix d'un SOC repose sur celui de ses fonctionnalités (la prévention, la détection, la réaction aux attaques) mais également sur des êtres humains et des outils qui doivent travailler de concert. Le SOC doit être adapté à son contexte car, s'il est mal raccordé avec ce dernier (infrastructure, gestion des incidents, CSIRT, etc.), son efficacité pour l'organisme sera amoindrie d'autant, a souligné Thierry Chiofalo, Responsable du Comité Conférences du CLUSIF, lors d'une conférence du Club le 7 décembre 2016. Le SOC est par ailleurs en évolution perpétuelle puisqu'il doit répondre à des menaces, un contexte métier, des risques et un contexte technique qui changent en permanence.

Pour Thierry Chiofalo, la mise en place d'un SOC s'intègre au processus de gestion du risque des systèmes d'information. Cette gestion du risque repose en effet, d'une part, sur des fonctions de pilotage qui permettent de contrôler l'efficience et les coûts des efforts consentis et, d'autre part, sur des fonctions de sécurité opérationnelle permettent de hausser effectivement le niveau de sécurité de l'organisme. Le SOC se rattache à ces fonctions opérationnelles et en constitue une brique importante.

Martine Guignard, secrétaire générale du CLUSIF et responsable du groupe de travail SOC a rappelé que celui-ci avait souhaité proposer un document « pragmatique » qui est le résultat de dix-huit mois de travaux. C'est un document neutre qui présente l'état de l'art dans ce domaine.

Le premier constat du groupe de travail a été qu'il existait très peu de documents de référence sur ce sujet, mis à part un document de la MITRE Corporation ou les référentiels PDIS et PRIS de l'ANSSI. Sur un plan marketing, les offres sont généralement peu claires et il n'existe pas de tarification précise.

Pour autant, il s'agit d'outils en plein essor et le CLUSIF souhaitait fournir un document non dogmatique qui puisse permettre aux DSI, RSSI ou Directeurs opérationnels de se faire une idée précise des étapes nécessaires au déploiement d'un SOC ainsi que de ses impacts dans l'entreprise.

Le document présente l'objectif d'un SOC, détaille l'organisation technique, mais aussi humaine, nécessaire. Il explore ensuite le catalogue des services et fonctions d'un SOC sur la base des quatre fonctions essentielles : prévention, détection, réaction et administration.

La prévention consistant à protéger le système d'information (SI) en renforçant les fondamentaux pour réduire les possibilités d'attaque. En ce qui concerne la détection, le SOC doit permettre de déceler toute attaque sur le périmètre du système d'information. Il doit être exhaustif et instantané dans la découverte des attaques contre le SI. Pour ce qui est de la réaction, le SOC doit assurer une prise en compte complète de l'attaque (périmètre, impact et temporalité). Si chacun peut positionner le curseur selon ses problématiques en matière de réponse, le SOC initie et participe à cette réaction aux attaques. Enfin, le SOC apporte une administration fonctionnelle des outils de sécurité avancés.

Le document produit par le groupe de travail évoque la mise en place du SOC, depuis la définition du projet et sa promotion en interne jusqu'à la mise en place et au bilan permettant de continuer à l'améliorer.

Martine Guignard a par ailleurs insisté sur la nécessité de l'identification précise des points de collecte des informations concernant les attaques. Certaines informations doivent être remontées, d'autres pas. Il ne s'agit pas d'être noyé sous un flux inexploitable d'alertes. Par ailleurs, des indicateurs sont nécessaires pour évaluer la maturité d'un SOC. La mise en place d'un SOC peut également générer des besoins en ressources humaines particulières comme des spécialistes des APT ou d'outils très spécifiques.

SOC Michelin : Quel bilan après 2 ans ?

Pierre RAUFAST, Michelin

Pierre Raufast, RSSI Europe et responsable du CERT Michelin a pour sa part présenté un retour d'expérience sur la mise en place du SOC dans son entreprise. Michelin compte 111 700 employés et est présent dans 170 pays.

« *Comme on externalise le SOC, on a tracé une ligne entre ce qu'on lui demande et ce que l'on garde comme prérogatives en interne* », a d'emblée précisé Pierre Raufast. « *Le SOC assure la collecte des informations et la détection de comportements suspects. Le CERT est le chef d'orchestre de la cyberdéfense du Groupe. Il définit les priorités de surveillance, assure la veille, la détection et la gestion des vulnérabilités, le traitement des incidents de sécurité en lien avec les parties prenantes*. »

Les deux entités doivent travailler main dans la main. Le maitre mot étant « collaboration » entre toutes les parties prenantes.

Le projet de SOC a débuté en 2013 chez Michelin, mais les premières alertes remontées datent de juillet 2014. Le CERT a quant à lui été créé au quatrième trimestre 2014. L'année suivante, le processus de gestion des incidents a été mis en place parallèlement à une montée en compétences et en moyens humains. En 2016, le CERT Michelin a obtenu sa certification tandis que le SOC s'agrémentait d'un processus de gestion de vulnérabilités.

Aujourd'hui, le SOC et le CERT fonctionnent convenablement. La gestion des incidents (tickets et faux positifs) est satisfaisante. La gestion de la veille est opérationnelle, chacun y participant. En ce qui concerne les opérations de forensic et l'expertise, Pierre Raufast souligne les résultats obtenus grâce aux outils et à la montée en compétence de l'équipe. Les processus et exercices de gestion de crise sont en place. La formation et la sensibilisation en interne fonctionnent convenablement. Quelques améliorations sont en revanche attendues pour ce qui est des scans et du patching afin de pouvoir aller au-delà des contraintes légales.

Enfin, Pierre Raufast a énuméré un certain nombre de facteurs de succès pour un projet de SOC et de difficultés à contourner.

- Il est important de connaître ses risques, savoir où regarder et qui est notre attaquant potentiel. Le degré de protection est une question de moyens financiers.
- Il faut également recruter et former, les compétences humaines étant importantes.
- Le top-management et le middle-management doivent être impliqués. Le SOC permet de fournir des exemples réels et concrets des dangers qui menacent l'entreprise.
- Le taux de faux positifs doit être rapidement maîtrisé afin d'éviter d'être noyé et de permettre au SOC d'apporter une réelle valeur ajoutée, a précisé Pierre Raufast.
- Enfin la relation avec le métier doit être claire, réactive et efficace.

Genèse d'un SOC multiniveau

Vincent Le TOUX, ENGIE

Vincent Le Toux, en charge des aspects de sécurité opérationnelle de Engie a pour sa part présenté le projet de SOC du groupe.

Celui-ci est très fortement décentralisé, compte 154 950 collaborateurs et des activités dans 70 pays.

Le premier projet de SOC du groupe est né en 2010 et n'a été actif qu'en 2012. Il apparaît dans le sillage du piratage d'une autre société du secteur de l'énergie en France. Il s'agissait d'un système permettant des scans de vulnérabilité couplé à un SIEM (Security Information & Event Management). La philosophie du projet était de voir ce que l'on trouverait dans les logs. Le modèle de financement reposait sur la refacturation par poste de travail et par serveur. En termes de résultats, le succès du SOC dans sa première

version a permis de dégager des résultats et d'identifier des points d'amélioration. Un des points relevés était la possibilité d'améliorer le traitement des incidents en renforçant l'implication des RSSI. Un autre était de revoir le modèle économique certain afin de tenir compte de la diversité des business units : certaines, par exemple, avaient peu de serveurs mais un gros trafic réseau. Par ailleurs, il existait dans le groupe des initiatives individuelles, parfois en raison d'obligations légales, parfois de participations spécifiques comme Cyberprotect (*via* Inéo). *In fine*, il a été décidé de tirer les leçons de cette expérience pour développer le SOC à travers un nouveau projet.

Un SOC version deux a donc vu le jour. Dix risques majeurs groupe ont été déterminés. L'approche a été *top down* et non plus *bottom up*. Une adaptation des risques suivant la business unit a été choisie en parallèle d'une priorisation des 25 sites industriels critiques du groupe. Le SOC fait l'objet d'une redevance systématique pour toutes les business units et elles sont donc encouragées à participer à son amélioration puisqu'elles payent pour ce service, quoi qu'il arrive.

Si une business unit dispose déjà d'un SOC, celui-ci est raccordé au SOC groupe. Si ce n'est pas le cas, le SOC du groupe vient couvrir les besoins.

Mise en œuvre et valeur ajoutée d'un SOC

Javier GONZALEZ, Airbus Defense & Space

Javier Gonzalez, expert SOC chez Airbus Defence and Space CyberSecurity a quant à lui apporté l'avis d'un offreur.

Pour lui, le SOC est un processus global de l'entreprise, il impacte l'ensemble de l'organisation et des métiers et nécessite une interaction entre toutes les parties prenantes.

La première question qui se pose est celle de la définition du périmètre de surveillance, précise Javier Gonzalez. Celui-ci est choisi en fonction des parties impliquées en interne, de la logique choisie, incrémentale ou exhaustive, des risques identifiés. Pour Javier Gonzalez, le plan de réaction doit être construit en même temps que le plan de protection.

Un Soc aide à assainir le système informatique et à sensibiliser les utilisateurs. S'il repère occasionnellement des APT, il remonte quotidiennement des attaques non ciblées, des faux positifs, mais aussi des problèmes liés à l'hygiène informatique des utilisateurs. Par exemple des administrateurs qui, utilisant massivement NMAP pour découvrir les services réseaux disponibles créent un bruit de fond parasite pour le SOC. Ou encore, des utilisateurs qui se servent d'outils de prise en main à distance de type Goto Webinar ou Webex non autorisés… Autre exemple vécu, les administrateurs qui réinitialisent leur mot de passe afin d'éviter de le changer.

Table ronde

Animée par Jean-Marc GREMY, Président du CLUSIF

Une session de questions-réponses a permis d'échanger avec l'auditoire. Il ressort un certain nombre de choses comme l'importance de la fermeture des incidents, ce qui permet de voir, à terme, si le SOC est pertinent. Le SOC peut par ailleurs donner des indications sur ce que les métiers font (ouverture d'un port pour le lancement d'une application par exemple). Pour l'ANSSI, le SOC est la seule réponse à la nouvelle menace contre les OIV. D'autant qu'il fournit les moyens techniques et humains pour trouver ce que l'on doit chercher quand il y a un incident Plusieurs représentants d'entreprise ont fait valoir les difficultés pour trouver les ressources humaines suffisamment qualifiées.