MOOC Supervision de Réseaux et Services

Transcription Interview 3
Thibault Coullet, Airbus Defence & Space
Equipe Supervision de la Sécurité

Présentation de l'équipe

Bonjour, je suis Thibault Coullet. Je vais vous parler de supervision de sécurité informatique. Pour parler de cela, je vais d'abord me présenter très rapidement. Je travaille chez Airbus. Chez Airbus, il y a une entité qui s'appelle Defence and Space, qui a une sous-division cyber-sécurité, dans laquelle je suis. Cette division est basée à Elancourt, près de Paris. Dans cette division se trouve un centre opérationnel de sécurité, qui s'occupe de superviser le réseau et les systèmes de différents clients. Qu'est-ce qu'un centre opérationnel de sécurité ? C'est un service dans lequel on opère pour le compte de différents clients, une supervision de sécurité. Notre rôle est d'identifier sur les réseaux et les systèmes des différents clients s'il y a une intrusion, qui mettrait à mal le système (ou les informations), ou des comportements plus ou moins malveillants sur le système (ou les réseaux). Dans ce centre opérationnel de sécurité, on trouve différentes équipes qui composent le SOC (Security Operations Center), principalement ce qu'on va appeler les niveaux 1 et 2, qui vont avoir des rôles un peu différents, mais globalement qui vont travailler ensemble pour détecter des intrusions et des comportements malveillants sur les systèmes.

Objectifs de la supervision

Pour réaliser une supervision de sécurité, on va avoir besoin de plusieurs choses. Déjà, quand on sera en face des outils, il faut qu'on soit capable de prioriser les événements et les incidents de sécurité. C'est une première étape. Pour prioriser les événements de sécurité, généralement, ce qu'on va faire, c'est afficher des couleurs ou des niveaux qui permettent de dire quel est l'incident le plus prioritaire par rapport à un autre. Une fois qu'on a réalisé cette priorisation des incidents de sécurité, il va falloir les analyser. Le deuxième besoin qu'on va avoir, c'est de pouvoir collecter les bons éléments techniques qui vont permettre de qualifier l'incident. Par exemple, si on a un malware qui est arrivé par voie de mail(s), il faut qu'on sache rapidement identifier qui est l'expéditeur du mail, qui est le destinataire, de quoi était composé le mail, qu'est ce qu'il y avait dans le corps du mail, est-ce qu'il y avait des liens internet ou des fichiers joints etc. Tous ces éléments, il faut les présenter facilement et rapidement à la vue de l'opérateur et des analystes. Une fois que tous ces éléments sont affichés, un besoin supplémentaire qu'il va y avoir, c'est quand on traite un incident de sécurité, on est souvent sur le coup du stress. Pour éviter de perdre du temps et de creuser des pistes qui n'aboutiront à rien, il est intéressant de toujours avoir une fiche réflexes à côté de soi, qui permet de bien vérifier qu'on respecte toutes les étapes de la méthodologie d'analyse, et qu'on n'oublie rien. Cette fiche est intéressante d'être gardée dans un outil, typiquement l'outil de supervision qu'on va utiliser, pour être présentée rapidement lors de l'analyse d'incidents. Chaque fiche correspond à un type précis d'incidents, et pourra ainsi être présentée dans le bon contexte avec la bonne méthode qui est adaptée à l'incident qu'on est en train de traiter. Une fois que tout ça est fait, on aboutit à un incident qui est

qualifié et sur lequel on sait dire si c'est un incident avéré ou c'est un faux positif. Une fois que tout ça est réalisé, le dernier besoin qui va être nécessaire de combler, c'est de savoir l'impact de cet incident. Pour mesurer l'impact d'un incident, il faut se rapprocher des clients ou d'une société (externe), ou de quelqu'un en interne dans l'entreprise, et savoir sur cette base de données (par ex.), quels sont les gens qui travaillent dessus, quels sont les métiers qui l'utilisent, est-ce que c'est une base de données importante, et est-ce qu'on va perdre beaucoup d'argent ou avoir un impact en terme de sensibilité des données important, s'il arrive quelque chose à ces données-là. Les outils, encore une fois, doivent être renseignés pour présenter ces informations de sensibilité et de criticité. Et c'est le dernier besoin, dont on va faire le tour ici, pour bien analyser et qualifier un incident de sécurité.

Méthodes et outils

Pour réaliser la supervision de sécurité, on va avoir besoin de méthodes et outils. Dans les outils, on va trouver classiquement différentes choses, tout le temps. Typiquement, si on s'intéresse à la partie réseaux, on va souvent voir des sondes de détection d'intrusions réseaux, d'autres équipements qui vont envoyer des informations, par exemple des firewalls ou des proxys qui sont en charge de relayer les connexions HTTPS vers l'extérieur etc. Tous ces éléments-là sont chargés, soit de détecter directement des intrusions, soit de loguer des informations d'audit et des informations spécifiques, qui vont pouvoir être ramenées dans le centre opérationnel de sécurité pour traitement. Suite à cela, on va pouvoir trouver d'autres types d'outils, qui vont être en charge de la collecte de tous ces événements de sécurité. Typiquement, il va y avoir plusieurs phases pour cette partie-là. Premièrement, la collecte des événements. Deuxièmement, on va filtrer ces événements pour ne garder que ce qui nous intéresse dans le cadre de la détection d'intrusions. Ensuite, on va extraire les données spécifiques qui nous intéressent dans ces événements-là, les ranger dans une base de données, et les corréler les uns avec les autres pour en extraire des comportements malveillants. Les outils qui font principalement cette tâche-là, c'est-à-dire de la collecte jusqu'à l'indexation dans la base de données, et la corrélation, sont les SIEMs. On peut en trouver différents, de différents constructeurs. Globalement, ils répondent tous à la même fonctionnalité : la collecte, l'indexation et la corrélation d'événements. Une fois qu'on a ces outils qui permettent de mettre en valeur des alertes et de lever des comportements suspects, on va utiliser un dernier type d'outils, qui vont être utiles pour traiter les incidents. Quand je dis traiter les incidents, ça veut dire se répartir les tâches d'analyse à effectuer dans toute l'équipe, savoir qui travaille sur quel incident, quels éléments d'analyse ont déjà été effectués ou non, chez quelle équipe sont les actions, est-ce qu'il y a une action dans l'équipe d'administration windows à faire pour la résolution d'incidents, ou est-ce qu'il y a une action dans l'équipe d'administration linux etc. Tout ça, ce sont les outils généralement qu'on appelle outils de ticketing, donc de gestion de tickets, qui vont être utilisés pour répondre à ces questions. Une fois qu'on a tous ces outils, on a la panoplie habituelle des outils qui vont être utiles au SOC, pour collecter les informations et traiter les incidents. Maintenant qu'on a ces informations-là, pour qualifier et analyser les incidents correctement, il va falloir qu'on s'appuie sur des méthodes. Les méthodes il y en a plein, et à plein d'endroits différents. On va principalement les trouver, soit décrites dans des normes, par exemple l'ISO 27001 ou l'ITIL, qui va nous donner quelques informations sur la manière dont gérer les incidents de sécurité, ou la manière de créer de nouveaux contrôles de sécurité pour détecter des incidents. Tout ça, ce sont des

normes qui vont permettre de créer toutes ces choses-là et de décrire des méthodes qui nous y aident. On va pouvoir aussi les retrouver évidemment dans différentes formations. Il y a plein d'organismes qui font les formations qui servent à apprendre des méthodologies d'analyse d'incidents, ou de forensics systèmes/réseaux, donc d'analyse sur différents types de systèmes ou réseaux. Ces méthodologies-là, on va pouvoir les utiliser pour faire l'analyse et la qualification des incidents de sécurité.

Métiers liés

Au sein d'un centre opérationnel de sécurité, on va trouver plusieurs types de personnes, qui ont plusieurs métiers. Principalement, ce qu'on va appeler les niveaux 1 et 2, qui sont en charge de la gestion d'incidents au jour le jour, vont avoir un profil principalement orienté expertise réseaux, c'est-à-dire que ce sont des personnes qui vont avoir un cursus réseaux et un peu de systèmes, et qui vont être capables de comprendre tout type de logs qui sont audités par différents types d'équipements, des firewalls, des proxys etc, qui vont pouvoir les interpréter, les comprendre, et les analyser. Donc, on a un premier profil, qui est de type experts réseaux. Ensuite, comme on va avoir affaire à beaucoup d'événements de plein de systèmes différents, il faut aussi quelques connaissances de base en systèmes, par exemple sur un système windows, ou un système linux, savoir où sont rangés les logs, ce qu'ils contiennent, qu'est ce qu'on peut trouver ou ne pas trouver dedans. C'est une deuxième expertise technique, qui est nécessaire sur les profils qu'on va trouver au sein du centre opérationnel de sécurité. Globalement, ce sont des profils qui sont un peu touche-à-tout, pas forcément très experts dans un domaine, mais qui ont une bonne connaissance de base sur de nombreux domaines, comme le réseau et le système. Une fois qu'on a fait le tour du SOC, et que l'équipe est complète avec ce genre de profils. De temps en temps, on peut se retrouver face à un incident qui nécessite une expertise. Pour résoudre ces problématiques-là, il y a des équipes d'experts spécialisés dans certains domaines, comme l'investigation numérique sur les systèmes, comme le reverse engineering de malwares et d'autres domaines d'expertise, qui vont pouvoir épauler les équipes du centre opérationnel de sécurité pour résoudre un incident particulier. On va pouvoir trouver les reversers de malwares, on va aussi pouvoir trouver des gens qui sont très experts sur, par exemple, les systèmes embarqués ou sur des systèmes à puce, comme des cartes bancaires etc. Pour chaque domaine d'expertise, on va pouvoir trouver une personne qui va pouvoir aider les gens du centre opérationnel de sécurité, afin de résoudre les incidents. Là, on a brossé un portrait à peu près complet des gens qui vont s'intéresser directement au traitement des incidents de sécurité. Mais, pour faire vivre un centre de ce type-là, on va avoir besoin d'autres profils, typiquement des gens qui vont développer les systèmes de détection. Chez Airbus, on a plusieurs solutions de sécurité qui sont développées ici-même. Les gens du centre opérationnel de sécurité discutent régulièrement avec les développeurs pour orienter les outils en fonction des besoins qu'on voit au jour le jour. Cela permet de mettre en valeur vraiment les événements, et tout ce dont a besoin l'opérateur pour faire une détection efficace. On a des développeurs, mais on va aussi trouver les intégrateurs de solutions de sécurité, qui vont pouvoir mettre en place tous les outils de détection, et le système de détection. On va trouver par exemple des architectes qui vont concevoir tout ce système, et pouvoir aider le centre opérationnel de sécurité à le déployer au bon endroit. Pour vous résumer, au sein du centre opérationnel de sécurité, on va plutôt trouver des profils techniques

qui savent faire de l'analyse réseaux et systèmes. Tout autour, on a de nombreux autres métiers qui gravitent et qui servent à faire un centre opérationnel de sécurité efficace.

Autres

Pour terminer, quelques points qui me semblent quand même assez importants à discuter. Le premier étant, qu'il est important d'être très curieux, si on veut travailler dans un centre opérationnel de sécurité, et plus globalement faire de la supervision de sécurité. C'est important dans tous les métiers, mais particulièrement dans celui-là, car ça vous apporte plein de choses, qu'on ne voyait pas jusqu'à maintenant. Si on se contente d'opérer les outils de façon classique, on va détecter des choses, mais beaucoup moins intéressantes, que si on avait appris concrètement comment s'en servir de manière avancée, et que la curiosité nous avait poussés dans les retranchements de chaque outil et de chaque information qu'on collecte. C'est vraiment une qualité exceptionnelle pour les gens qui travaillent dans ce milieu-là. Cela peut avoir aussi d'autres représentations. Par exemple, quand je parlais tout à l'heure des différentes équipes, qui tournaient autour du SOC et qui arrivent à l'alimenter correctement et à le configurer correctement. C'est la curiosité qui pousse à aller voir toutes ces équipes-là. Donc, ça peut être les intégrateurs, qui vont configurer les outils, les auditeurs qui vont aller sur le terrain faire des audits de sécurité et qui vont rapporter de l'information intéressante pour la supervision. Cela peut être les équipes de réponses à incidents, qui vont aller sur le terrain quand il y a un problème, et qui vont ramener encore plus de contexte qu'avant. Donc, cette curiosité, elle se traduit vraiment dans les échanges avec les différentes équipes, qui tournent autour du SOC, et qui sont en contact privilégié avec le client, qui vont pouvoir apporter de nouveaux éléments pour améliorer la supervision et la détection. Cela peut se traduire d'une dernière manière aussi, en terme de veille. On est dans un contexte où les informations, les systèmes et les outils évoluent tous les jours. Donc, si on ne se tient pas au courant, on est vite dépassé par les événements. C'est extrêmement important d'être curieux, je le redis encore une fois, mais surtout de faire de la veille sur tout ce qui est outils et menaces. Sans quoi, on va vite être dépassés par les techniques de piratage et d'intrusion. Cela serait vraiment dommage de ne pas être au courant de quelque chose qui est largement discuté dans la sphère publique et qu'on n'aurait pas pu détecter, parce qu'on n'était juste pas au courant que c'était en train de se passer. La veille est vraiment aussi un élément important à garder en tête, quand on fait la supervision de sécurité. Pour finir, je vais parler du traitement des données. Comme vous pouvez l'imaginer, il y a énormément de données, qui arrivent dans un SOC. Etre curieux ce n'est pas tout, il faut aussi être méthodique. Si l'on n'a pas une certaine méthodologie et un certain recul pour prioriser les tâches et les incidents, qu'on ne s'est pas bien fixé une méthodologie ou plusieurs, qu'on ne les a pas écrite(s) et gardée(s) à proximité, cela va être très difficile d'appréhender toutes les informations qui arrivent, et de pouvoir les traiter correctement. Bien garder en tête, comme on l'a dit précédemment, que la méthodologie, c'est quelque chose d'important à voir et qui va servir pour vraiment faire une supervision de qualité et efficace.