Orchestration et renseignement sur les menaces : le moteur et son carburant

La prévention s'accompagne désormais de la détection et de la réponse à incident et les entreprises étudient la possibilité d'employer des outils d'orchestration, d'automatisation et de réponse de sécurité (Security Orchestration, Automation and Response, SOAR).
D'après le guide des solutions SOAR de Gartner, d'ici la fin 2022, 30 % des entreprises dont l'équipe de sécurité compte plus de cinq personnes exploiteront des outils SOAR dans le cadre de leurs activités de sécurité, contre moins de 5 % en 2019.

De nombreux facteurs stimulent la demande, en premier lieu la pénurie de talents qualifiés dans le domaine de la cybersécurité, qui force la plupart des entreprises à trouver des moyens d'automatiser les tâches répétitives.

Le rôle des outils d'orchestration

Les outils d'orchestration, en particulier les playbooks, sont utiles pour automatiser les processus dont il est avéré que l'exécution ne présente aucune variante. Le système réagissant par réflexe, le besoin d'intervention humaine dans ces cas est limité. Les playbooks aident les équipes en charge de la résolution des incidents à accélérer les interventions et à atténuer les risques, tout en permettant aux ressources spécialisées de se concentrer sur des tâches à plus forte valeur ajoutée, ce qui contribue également à fidéliser les équipes.

Le rôle du service de renseignement sur les menaces est différent : il consiste à recueillir des données sur les menaces et les événements externes et internes, à les normaliser pour les analyser et à les évaluer et les hiérarchiser automatiquement selon des critères propres à l'entreprise. Avec une plate-forme servant de référentiel central, les équipes et outils ont accès à l'historique des investigations, observations et enseignements de l'entreprise concernant les adversaires et leurs tactiques, techniques et procédures. Au fil de l'ajout de nouvelles données et de nouveaux enseignements, la plate-forme réévalue et reclasse automatiquement les renseignements pour améliorer les opérations de détection, d'investigation et de réponse en cours.

Un travail de concert pour accélérer la détection et la réponse

Les outils d'orchestration et la plate-forme de renseignement sur les menaces répondent au même objectif global : faire gagner du temps, pour que les humains puissent se concentrer sur les domaines qui requièrent leur intelligence, leur expérience et leurs compétences, et s'épargnent les tâches pouvant être facilement automatisées. Ces outils sont encore plus efficaces lorsqu'ils fonctionnent de concert.

À vrai dire, il est possible d'en faire davantage pour optimiser les playbooks afin d'obtenir un gain

de temps exponentiel. Orienté par le renseignement sur les menaces, un outil d'orchestration peut identifier les liens et les tendances, et ajuster l'exécution des playbooks pour optimiser l'efficacité. Et lorsqu'une plate-forme de Cyber Threat Intelligence sur les menaces tire parti des enseignements issus de la pratique de la réponse aux incidents, elle peut bénéficier d'un contexte plus large pour accélérer la détection et la réponse.

Prenons comme exemple une campagne de phishing dans laquelle une entreprise a été ciblée par 100 e-mails. Le playbook signale un élément inconnu, le transmet à un outil d'inspection qui confirme qu'il est suspect, puis l'envoie à une sandbox qui valide le fait qu'il s'agit d'un malware.
Le fichier est ensuite ajouté à la liste de blocage par réputation. À la réception d'un nouvel e-mail suspect, le playbook répète l'opération. Au fil du temps, la liste de réputation s'allonge et les performances système sont ralenties à force de devoir répondre constamment aux mêmes requêtes.

Cependant, si l'outil d'orchestration fonctionne de concert avec la solution de renseignement sur les menaces, il devient inutile d'exécuter l'ensemble du playbook à chaque fois.
La plate-forme mémorise les activités de la même famille et campagne de malware, reconnaît qu'il s'agit d'une menace immédiate et réelle pour l'entreprise et applique une notion de scoring (allant de 1 à 10) – pour le cas présent une note de 9 ou 10. Le playbook peut être rédigé de manière à ajuster les processus en fonction de la notation. Par exemple, une note de 7 à 10 pourra déclencher un blocage automatique, une note de 3 à 7 envoyer le fichier directement vers la sandbox et une note inférieure déclencher le playbook complet. La capacité des playbooks à s'ajuster de manière dynamique en fonction des scores renforce l'efficacité des outils et des équipes.

La gestion des listes de réputation est un autre aspect qui s'améliore lorsque l'orchestration et le renseignement sur les menaces fonctionnent de concert. L'outil d'orchestration n'a pas pour responsabilité de tenir à jour la liste de réputation, qui peut très vite devenir ingérable.
En revanche, une plate-forme de CTI suit et stocke les données sur les menaces et événements provenant de tous les groupes et sources, et mémorise ce qu'elle a vu, ce qui lui permet de cerner le cycle de vie d'une menace et de savoir à quel moment elle peut être éliminée de la liste de réputation. En supprimant celles obsolètes, de nouvelles informations peuvent être ajoutées sans risquer de surcharger la liste de réputation.

L'outil d'orchestration consiste à exercer un réflexe, tandis que la pratique du renseignement sur les menaces consiste à exercer la mémoire. Bien que leurs approches soient différentes, les outils d'orchestration et les plates-formes de threat intelligence partagent le même objectif : accélérer la détection, la réponse et l'atténuation des risques. Et lorsqu'ils fonctionnent de concert, ils font gagner du temps aux équipes, et leurs résultats n'en sont que meilleurs.