Threat Intelligence : du renseignement d'intérêt cyber au Hunting

Les plateformes de gestion de Cyber Threat Intelligence, conçues initialement pour palier à l'hétérogénéité et à la volumétrie des sources externes de renseignement sur les menaces ont joué un rôle de normalisation des flux externes et d'automatisation de leur consommation au sein des SOC (et particulièrement des SIEM).

Cependant, cet usage à l'origine très opérationnel n'a cessé d'évoluer et les plateformes de gestion du renseignement endossent désormais un rôle beaucoup plus global et transverse.
Cela est notamment dû à la prise de conscience générale du fait que les sources les plus importantes pour la sécurité des entreprises sont internes et correspondent au renseignement généré par les différents services en place (détection, réponse, gestion des vulnérabilités, SecOps, risque, fraude, ...).
En effet, la prise en compte de ces sources a donné des perspectives différentes aux entreprises et a propulsé les plateformes de gestion du renseignement dans une fonction nouvelle.

Fusion Center : vers un partage automatique et structuré de l'information

Nos organisations fonctionnent en silos : la détection (au sein d'un ou de plusieurs SOC, parfois externalisés), la réponse aux incidents (au sein d'un CSIRT ou d'un CERT), la gestion des vulnérabilités, l'outillage EndPoint, la prévention périmétrique (en charge de la politique de réputation) ...
Ce sont autant de départements possédant leurs propres outils, équipes et processus spécifiques, mais qui ne communiquent entre eux que de manière limitée. Le principe même de distribution des rôles par silos a tendance à générer de la perte d'information.

Le concept de Fusion Center propose une compétence novatrice et très efficace : faire en sorte que chaque leçon apprise par un homme ou une machine d'un de ces départements puisse nourrir en temps réel tous les autres départements (hommes ou machines) pour leurs prises de décisions et la priorisation de leurs actions.

Le but n'est donc pas ici de casser les silos, mais de mettre en place un processus de partage automatique et structuré de l'information entre eux.

Chaque département avait déjà élaboré une capacité de capitalisation sur son travail, il s'agit de capitaliser de manière transverse et globale afin d'améliorer l'efficacité de tous.
Chaque élément de capitalisation d'un département est alors considéré comme un renseignement d'intérêt cyber dont la source est interne (SOC, CSIRT, SECOPS...).
L'utilisation de ce renseignement interne comme prisme de consommation des flux externes permet de prioriser le renseignement contextuel à l'entreprise et de distribuer à l'ensemble des départements les objets et rapports dont ils ont besoin au quotidien.

Ainsi, au sein d'un Fusion Center, la plateforme de gestion du renseignement joue un rôle double de « bus » de communication entre silos (usage opérationnel) et de mémoire centrale des menaces constatées par l'entreprise (usage stratégique). L'analyse du contenu de cette mémoire permet ensuite d'envisager d'autres usages.

L'orchestration, remède contre la perte de temps

La plupart des organisations travaillent actuellement sur la notion d'orchestration rendue possible par les outils spécialisés récents. L'idée est de déléguer à l'orchestrateur le traitement de l'ensemble des tâches évidentes et répétitives afin de permettre aux analystes des pôles détection et réponse de se concentrer sur les tâches nécessitant une réflexion et un jugement humain. Le traitement de volumes importants de courriers d'hameçonnage est un bon exemple d'application de ce concept.

Ainsi, l'utilisation du « bus » de communication (mémoire centrale des menaces – plateforme de renseignement) par l'orchestrateur semble évidente pour lui permettre de dérouler ses playbooks en fonction du renseignement collecté par l'entreprise. Il pourra traiter des centaines de courriers d'hameçonnage en quelques minutes sans requérir l'intervention humaine dans le déroulement de son playbook dédié à ce thème. Autant de temps gagné par les analystes (c'est bien là l'objectif principal).

Cependant, la délégation de telles tâches auprès de l'orchestrateur ne peut pas se faire au détriment de la capitalisation. Il est important de faire en sorte que l'orchestrateur soit un contributeur actif de capitalisation auprès de la plateforme de renseignement.

En effet, cette contribution va permettre à la plateforme de gestion du renseignement d'identifier la campagne associée aux courriers d'hameçonnage, d'identifier l'adversaire, de réaliser qu'un seul département est ciblé au sein de l'entreprise, de comprendre le calendrier des envois de courriers, de mettre en lumière les techniques et tactiques associées à l'intrusion initiale d'hameçonnage et de faire apparaître ces informations dans un tableau de bord pour alerter les analystes sur ces attaques ayant été intégralement traitées jusqu'alors de manière automatisée…

L'analyse humaine de l'ensemble de la vague subie est probablement nécessaire.

Ainsi, l'orchestration est indissociable de la gestion du renseignement et les deux fonctions s'alimentent l'une et l'autre. Les projets d'orchestration de réponse aux incidents ayant tendance à accélérer l'utilisation transverse des plateformes de gestion du renseignement d'intérêt cyber.

Gestion du renseignement : point de départ du Hunting

Alimentée par les sources de renseignement externes et les sources internes issues des différents départements, la plateforme de gestion du renseignement devient un outil privilégié pour réaliser une analyse précise de la menace prioritaire pour l'entreprise. Facilitée par l'intégration de Frameworks spécialisés (Mitre ATT&CK étant actuellement le plus utilisé), cette analyse permet

d’avoir accès aux techniques et tactiques détaillées utilisées par les adversaires constatés.

La plateforme devient alors le point de départ du Hunting pour l’entreprise, lui permettant de faire les suppositions nécessaires et préalables à tout démarrage de campagne afin d’optimiser ses ressources.