RAPPORT DE SYNTHÈSE

Déstabiliser les fauteurs de troubles, art ou science ?

Services financiers

En savoir plus

Pour lire le rapport complet, consultez la page suivante : **www.mcafee.com/fr/solutions/lp/evolution-soc.html**

Dans le secteur des services financiers, les professionnels de la sécurité luttent au quotidien pour traquer les attaques qui menacent de perturber leur organisation ou de dérober des données. Bien que l'effet de surprise joue presque toujours en faveur des auteurs d'attaques, une traque efficace des menaces permet de les déstabiliser. Si les entreprises de services financiers disposent des outils nécessaires pour contrer ces attaques, les résultats obtenus ne sont pas toujours probants. Plusieurs facteurs sont mis en cause, tels que le manque d'effectifs à temps plein spécialisés dans la traque des menaces, la sous-utilisation des outils et une prédominance des processus par rapport à l'intuition humaine.

Cette analyse de la traque des menaces au sein des services financiers s'appuie sur l'étude 2017 de McAfee sur la traque des menaces, *Déstabiliser les fauteurs de troubles, art ou science ?* L'étude a été menée à l'échelle internationale, auprès de professionnels de la sécurité et de l'informatique travaillant dans des entreprises de taille intermédiaire (1 000 à 5 000 personnes) ou des grandes entreprises (plus de 5 000 personnes).

Gardez le contact

Le degré de maturité des opérations de traque des menaces au sein de l'entreprise a constitué une variable essentielle pour l'analyse des résultats. Allant du niveau 0 (Initial) au niveau 4 (Expert), ces auto-évaluations offrent des informations précieuses sur la nature actuelle de la traque des menaces et aident les entreprises à cerner et à améliorer leurs capacités dans ce domaine.

Principales observations

- Dans le secteur des services financiers, les responsables de la traque des menaces opèrent en moyenne dans un environnement de degré de maturité 2, ou légèrement en deçà. Ce type d'environnement se caractérise par une prédominance des processus, une sous-utilisation des principaux outils de traque et des difficultés de gestion des grands volumes de données de sécurité générés.
- Les entreprises les plus avancées en matière de traques des menaces sont deux fois plus susceptibles que les entreprises de services financiers d'automatiser des étapes du processus d'investigation des attaques. Elles sont également plus susceptibles (+20 %) de disposer d'une équipe à temps plein spécialisée dans la traques des menaces ; elles parviennent ainsi à déterminer les causes des incidents dans 74 % des cas, contre une moyenne de 58 % dans les services financiers.
- Les experts de la traque des menaces utilisent un large éventail d'outils pour arriver à leurs fins. De leur côté, les entreprises de services financiers n'exploitent qu'une fraction des outils à leur disposition, sous-utilisant de ce fait les environnements sandbox, les technologies de leurre, les scripts personnalisés et les outils d'analyse du comportement des utilisateurs.
- Les entreprises de services financiers disposent bien des outils nécessaires, mais pas du personnel requis pour les utiliser efficacement. Elles affectent en moyenne six collaborateurs à la traque des menaces, soit un peu moins de la moyenne établie à sept, mais bien en deçà des neuf experts que l'on retrouve dans les entreprises de niveau 4.
- D'une manière générale, les outils privilégiés varient selon le degré d'expérience. Le plus apprécié par les analystes de niveaux 1 et 2 (quels que soient la taille et le niveau de maturité du SOC) est le sandbox, alors que leurs homologues de niveaux 3 et 4 utilisent ce dernier au sein d'un éventail plus large d'outils. Au sein des entreprises de services financiers, les analystes de niveau 1 affichent une trop grande dépendance aux technologies EDR (Endpoint Detection and Response). Les analystes de niveau 2 possèdent une expérience supérieure à la moyenne en matière de scripts personnalisés. Parallèlement, leurs analystes de niveaux 3 et 4 signalent une sous-utilisation de quasiment tous les outils de traque, notamment des environnements de sandbox (niveau 3) et des technologies EDR (niveau 4).
- La personnalisation et l'optimisation sont fondamentales. Dans les SOC matures, l'effectif chargé de la traque des menaces consacre 30 % de temps en plus à la personnalisation des outils et techniques. Il recourt massivement à des solutions de gestion des événements et des informations de sécurité (SIEM) et à des scripts personnalisés pour automatiser les processus manuels et ad hoc.
- La cyberveille a un impact significatif sur les résultats. Les entreprises les plus matures utilisent des indicateurs de compromission à des fins de validation et d'amélioration du processus décisionnel, à tous les niveaux de l'architecture de sécurité. Parmi les meilleures pratiques, citons l'étude des tactiques,

techniques et procédures des auteurs d'attaques, le développement de compétences d'observation et l'enrichissement des données de cyberveille par leur collecte auprès des sources pertinentes.

Observer, s'orienter, décider et agir

La prise de décision par l'être humain peut jouer un rôle déterminant dans de nombreux scénarios de sécurité et faire pencher la balance en votre faveur. Alors qu'il servait dans l'Armée de l'air américaine, le colonel John Boyd a été le premier à documenter les quatre phases fondamentales de ce processus, à savoir observer, s'orienter, décider et agir (boucle OODA). Les équipes de sécurité performantes mettent cette approche à profit pour exploiter les faiblesses de leurs adversaires, avec le soutien de processus automatisés, de fonctions d'analyse et de données de cyberveille. Les responsables de la traque des menaces partent souvent de l'hypothèse qu'une intrusion ou une compromission s'est produite. Ils suivent des indices et leur intuition personnelle, puis transforment les procédures éprouvées en règles automatisées.

D'après les résultats de l'étude, les responsables de la traque des menaces au sein d'entreprises de services financiers opèrent dans un environnement de degré de maturité 2. À ce niveau, la traque des menaces passe d'une tâche ponctuelle à une activité plus axée sur les processus, pour parvenir au final à un juste équilibre entre interventions ad hoc et processus dans les équipes les plus évoluées. À mesure qu'elles gagnent en maturité, les équipes affinent leurs processus et leurs techniques de traque tout en faisant appel à l'automatisation et aux fonctions d'analyse pour faciliter la gestion des gros volumes de données de sécurité. Les entreprises de services financiers disposent généralement d'un niveau d'automatisation supérieur à la moyenne dans la

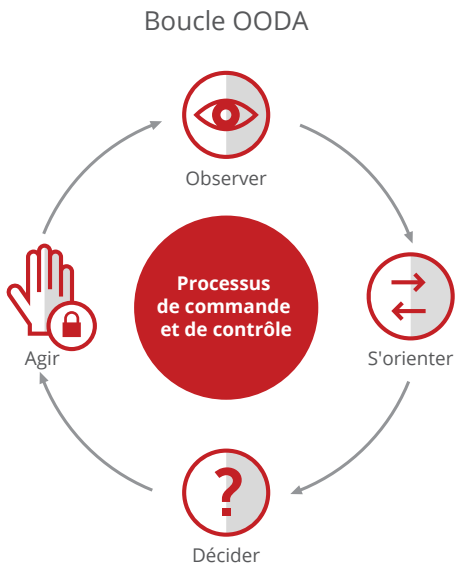

Figure 1 : Boucle OODA.

plupart des domaines, exception faite de la réponse aux incidents. Néanmoins, il semblerait qu'elles n'exploitent que rarement les nombreux outils à disposition et qu'elles éprouvent des difficultés à gérer les grands volumes de données générés. Pourtant, leur taux d'utilisation de l'outil de gestion des Big Data Hadoop est parmi les plus bas, soit 25 % inférieur à la moyenne.

Les entreprises de niveau 2, pour lesquelles la traque des menaces reste une activité à temps partiel, estiment que leur principale priorité est d'embaucher plus de personnel expérimenté. On remarque en outre que les entreprises de services financiers donnent la priorité à une meilleure intégration de leurs capacités de traque des menaces au sein des SOC, suivie d'une meilleure automatisation et d'une meilleure formation du personnel. La formation du personnel est particulièrement importante, car le

phishing apparaît comme l'origine principale des menaces identifiées pour ce groupe.

Conclusions

Lorsque les entreprises gagnent en maturité, elles documentent les étapes reproductibles de l'investigation des attaques, ce qui ouvre la voie à une automatisation plus systématique. Au niveau 2, moins de 45 % des processus sont automatisés, alors que ce pourcentage dépasse 70 % au niveau 4. L'adoption de l'automatisation, pour peu qu'elle soit associée à une identification compétente et efficace des schémas comportementaux anormaux, produit une synergie entre la traque des menaces et la réponse aux incidents. Celle-ci a pour effet d'accélérer le tri des incidents, de réduire les délais de résolution et d'améliorer l'identification des causes sous-jacentes. De fait, l'enquête révèle que plus de 70 % des SOC matures clôturent les investigations dans un délai moyen inférieur à sept jours, contre un délai de trois semaines pour les entreprises de niveau 2. Ils parviennent à déterminer les causes des incidents dans 70 % des cas, contre seulement 58 % des cas pour les services financiers.

Les équipes de traque des menaces disposent d'un large éventail d'outils et de techniques pour détecter, confiner et neutraliser les cyberattaques, mais ceux-ci sont sous-utilisés dans les services financiers. Ce scénario est très répandu dans les entreprises de niveau 2, car elles ont parfaitement conscience qu'adopter de nouveaux outils sans repenser d'autres aspects ne peut produire des résultats positifs.

« Cette enquête souligne un point important : les entreprises matures pensent en premier lieu à développer leurs capacités pour atteindre un résultat, puis identifient les technologies et les processus qui leur permettront d'y parvenir. Les autres, par contre, veulent d'abord acquérir les moyens technologiques et se concentrent ensuite sur le résultat. »

Mo Cashman, Architecte de solutions d'entreprise et Ingénieur en chef, McAfee

Le sandboxing, l'automatisation et l'analyse peuvent se mettre au service des équipes de traque des menaces moins expérimentées. Toutefois, les entreprises qui n'ont pas investi dans leur architecture ni défini de processus pour soutenir cette automatisation n'obtiendront pas les effets espérés. À mesure qu'elles gagnent en maturité, elles deviennent plus performantes grâce à l'alliance de l'homme et de la machine, mêlant l'intuition et le jugement du premier à la rapidité de traitement et aux capacités de reconnaissance de modèles de la seconde.

La traque des menaces n'est pas un phénomène de mode. De même, il ne s'agit plus d'une démarche ésotérique limitée à une poignée d'experts avant-gardistes. Dans les prochaines années, il faut s'attendre à ce qu'elle fasse partie intégrante des opérations de sécurité axées sur l'analyse dans la plupart des entreprises, et qu'elle soit soutenue par une automatisation poussée et des analyses basées sur l'apprentissage automatique.

À propos de McAfee

McAfee est l'une des plus grandes entreprises de cybersécurité indépendantes au monde. Convaincue de l'efficacité de la collaboration, McAfee met au point des solutions pour particuliers et pour entreprises conçues pour rendre nos environnements plus sûrs. www.mcafee.com/fr

McAfee
Together is power.

11-13 Cours Valmy - La Défense 7
92800 Puteaux, France
+33 1 4762 5600
www.mcafee.com/fr

3741_0118
JANVIER 2018