RAPPORT DE SYNTHÈSE

Déstabiliser les fauteurs de troubles, art ou science ?

Industrie manufacturière

En savoir plus

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

Dans le secteur manufacturier, les professionnels de la sécurité sont confrontés à de nombreux défis pour protéger les machines connectées et l'importante surface d'attaque de leurs entreprises. 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 manufacturières disposent des outils adéquats, elles enregistrent des résultats inférieurs à la moyenne en matière d'analyse des causes fondamentales et de délai de résolution des incidents. Leurs principales difficultés semblent être liées au personnel, car leurs effectifs impliqués dans la traque des menaces sont parmi les plus bas et la formation dans ce domaine ressort comme leur principal problème.

Gardez le contact

Cette analyse de la traque des menaces dans le secteur manufacturier 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).

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 manufacturier, les responsables de la traque des menaces opèrent en moyenne dans un environnement de degré de maturité 2 ou 3, ou en tout cas de niveau moyen. Dans ce type d'environnement, la traque des menaces est davantage axée sur l'équilibre entre interventions ponctuelles et processus, plutôt que sur les processus seuls. L'accent est mis sur l'automatisation des tâches, les recherches et la personnalisation des outils.
- Les entreprises les plus avancées en matière de traques des menaces sont deux fois plus susceptibles que les entreprises manufacturières 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 traque des menaces ; elles parviennent ainsi à déterminer les causes des incidents dans 74 % des cas, contre une moyenne de 52 % seulement dans l'industrie manufacturière.
- Les experts de la traque des menaces utilisent un large éventail d'outils pour arriver à leurs fins. Si les entreprises du secteur manufacturier évoluent dans cette direction, elles sous-utilisent encore certaines solutions telles que les outils à code source libre et les analyses avancées. De même, elles restent sans doute trop dépendantes des outils de gestion des Big Data comme Hadoop.
- Les entreprises manufacturières 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. Les entreprises du secteur manufacturier déplorent une sous-utilisation des solutions SIEM et EDR par leurs analystes de niveau 1, ainsi qu'une sous-utilisation des environnements de sandbox et des outils d'analyse du comportement des utilisateurs par leurs analystes de niveau 4.

- La personnalisation et l'optimisation sont fondamentales. Dans les SOC matures, l'effectif chargé de la traque des menaces consacre 20 % de temps en plus à la personnalisation des outils et techniques que dans les entreprises du secteur manufacturier. Il recourt massivement à des solutions 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

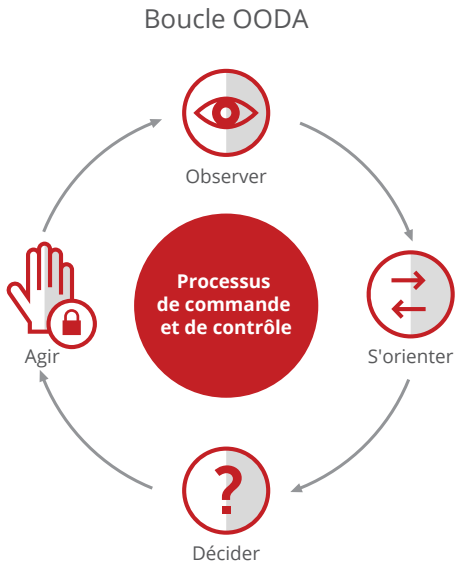

Figure 1 : Boucle OODA.

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 des entreprises manufacturières opèrent dans un environnement de degré de maturité 2 ou 3. À ces niveaux, 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 du secteur manufacturier disposent généralement d'un niveau d'automatisation acceptable dans la plupart des domaines, mais passent sous la moyenne pour ce qui est de l'automatisation des tâches correctives. Si leur défi principal est vraisemblablement la formation des responsables de la traque des menaces, ces entreprises rencontrent également des difficultés en matière de validation des données et de traitement des indicateurs de compromission. Le manque de correctifs pour systèmes d'exploitation apparaît comme la cause fondamentale des menaces dans une proportion sensiblement supérieure à la moyenne. Elle s'avère responsable de 53 % des attaques, contre seulement 39 % pour le reste du groupe.

Les entreprises de niveaux 2 et 3, pour lesquelles la traque des menaces devient une activité à temps plein, estiment que leur principale priorité est d'embaucher plus de personnel expérimenté. Pour leur part, les entreprises manufacturières placent le besoin d'outils de diagnostic plus précis en tête de liste, à quoi viennent s'ajouter le recrutement de personnel plus expérimenté et une meilleure automatisation.

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 et un délai de 15 jours dans le secteur manufacturier. D'autre part, le groupe des SOC matures parvient à déterminer les causes des incidents dans 70 % des cas, contre seulement 52 % des cas pour les entreprises manufacturières.

Les équipes de traque des menaces disposent d'un large éventail d'outils et de techniques pour détecter, confiner et neutraliser les cyberattaques, et ceux-ci progressent vers une utilisation optimale dans l'industrie manufacturière. 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

3742_0118
JANVIER 2018