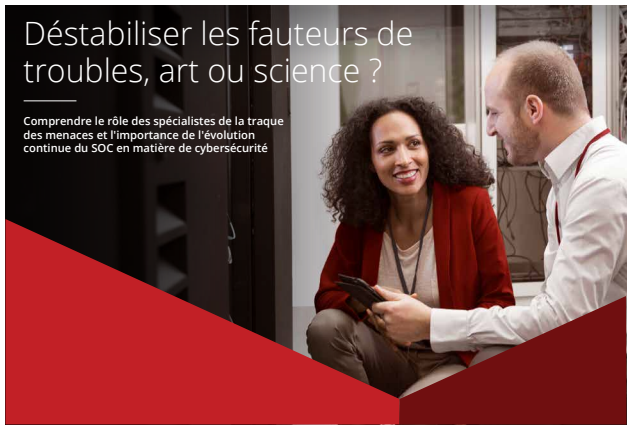
RAPPORT DE SYNTHÈSE

Déstabiliser les fauteurs de troubles, art ou science ?



En savoir plus

Pour lire le rapport complet, consultez la page suivante : **mcafee.com/soc-evolution**

Résumé

Les professionnels de la sécurité luttent chaque jour pour traquer des cybercriminels qui cherchent à perturber les activités de leur entreprise. Bien que l'effet de surprise joue presque toujours en faveur des auteurs d'attaques, une traque efficace des menaces permet de les déstabiliser.

McAfee a réalisé une enquête auprès de plus de 700 professionnels de la sécurité et de l'informatique travaillant dans des entreprises de taille intermédiaire (effectif compris entre 1 000 à 5 000 personnes) ou des grandes entreprises (plus de 5 000 personnes) dans le monde. L'objectif était de dégager des informations et des enseignements utiles pour les entreprises soucieuses de mieux cerner et d'améliorer leurs capacités de traque des menaces.

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 révèlent quelques surprises quant à la façon dont les entreprises investissent pour s'améliorer.

Principales observations

- Les équipes de traque de menaces les plus avancées sont deux fois plus susceptibles d'automatiser des étapes du processus d'investigation des attaques et consacrent 50 % de temps en plus à la traque effective. Par conséquent, 70 % d'entre elles clôturent les investigations en moins d'une semaine, contre seulement 50 % dans les entreprises à la traîne.
- Les entreprises matures sont trois fois plus nombreuses à considérer que chaque étape des processus d'identification et d'investigation peut être automatisée, en particulier l'analyse en environnement sandbox, la détection et la réponse aux incidents pour les terminaux et l'analyse du comportement des utilisateurs.
- 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 peu matures tentent d'exploiter les mêmes technologies que celles arrivées à maturité, sans toutefois obtenir les mêmes résultats. L'adoption de nouveaux outils suffit rarement si les processus de prévention des menaces et de réponse aux incidents n'évoluent pas. En effet, les équipes ne seront jamais réellement efficaces sans un investissement initial dans l'architecture et des processus optimisés.
- La personnalisation et l'optimisation sont fondamentales. Dans les SOC matures, l'effectif chargé de la traque des menaces consacre 70 % 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.
- L'exploitation de la cyberveille a un impact significatif sur les résultats. Les entreprises plus matures utilisent les indicateurs de compromission à des fins de validation des menaces 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 (TTP) 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 (cycle 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. La traque des menaces se concentre sur l'humain tout en faisant appel à un grand éventail d'outils et de renseignements pour identifier les menaces cachées qui ciblent l'entreprise.

Les résultats de l'enquête révèlent que, dans les entreprises les moins matures, la traque des menaces débute sous la forme d'une procédure ponctuelle. Ensuite, l'accent est mis davantage sur le développement des processus, pour parvenir au final à un juste équilibre entre interventions ad hoc et processus dans les équipes les plus évoluées. Les entreprises à la traîne ont tendance à submerger leurs équipes de traque de menaces de données et d'outils sophistiqués — avec peu de succès. 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. Une fois parvenues au niveau 4, les équipes de traque des menaces sont bien plus efficaces. Elles utilisent les données et les outils de façon sélective, en veillant à ce qu'ils soient adaptés à l'environnement et aux vecteurs d'attaque potentiels.

À eux seuls, les moyens humains ne permettent pas de prendre en charge le volume élevé des données de sécurité. Pour la plupart des entreprises, la gestion de ces données et leur exploitation à des fins de validation des menaces constituent les deux difficultés majeures. Les entreprises moins matures peinent à accéder aux données et à prioriser les événements, alors que les plus matures considèrent que la validation des menaces constitue le plus grand défi. Il n'est pas étonnant que les entreprises de niveaux 1 et 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. Dans les entreprises plus matures, une meilleure automatisation et l'utilisation accrue de l'analyse arrivent en première et deuxième positions. En effet, l'objectif n'est alors plus de bâtir des équipes solides pour pister les menaces et répondre aux incidents, mais plutôt de les rendre plus efficaces.

Boucle OODA

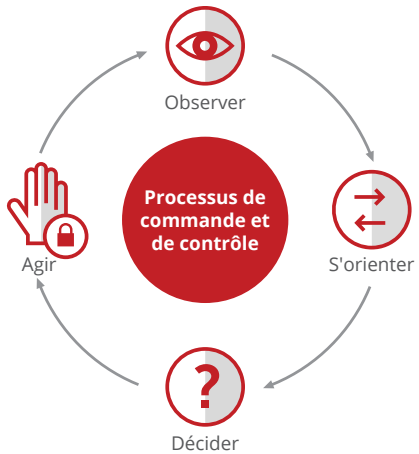


Figure 1 — Boucle OODA

Conclusion

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 1, seuls 40 % 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 ingénieuse et efficace des schémas comportementaux anormaux, produit une synergie entre la traque des menaces et la réponse aux incidents, avec pour effets 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 de moins de 7 jours et parviennent à déterminer les causes des incidents dans 70 % des cas, contre un délai de 25 jours et seulement 43 % des cas pour les SOC les moins matures.

71 %

des SOC ayant atteint le niveau 4 de maturité mènent à bien les investigations des incidents en moins d'une semaine.

Les équipes de traque des menaces recourent à un large éventail d'outils et de techniques pour détecter, confiner et neutraliser les cyberattaques. 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.

Néanmoins, calquer les outils et techniques des experts en traque des menaces ne suffit pas. Pour les entreprises à la traîne, l'adoption de nouveaux outils sans repenser d'autres aspects ne peut produire des résultats positifs. Le sandboxing, l'automatisation et l'analyse peuvent se mettre au service des équipes de traque des menaces moins expérimentées, mais les entreprises qui n'ont pas investi dans leur architecture ni défini de processus pour soutenir cette automatisation n'obtiendront pas les effets espérés.

« 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, en revanche, 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

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 de la plupart des entreprises et qu'elle soit soutenue par une automatisation poussée et des analyses automatiques.

À propos de McAfee

McAfee est l'une des plus grandes entreprises de cybersécurité indépendantes au monde. Inspirée par la puissance de la collaboration, McAfee crée des solutions pour entreprises et particuliers qui contribuent à un monde plus sûr. www.mcafee.com/fr

McAfee Together is power.

McAfee Ireland Ltd.
Building 2000, City Gate
Mahon, Cork, Ireland
www.mcafee.com/fr