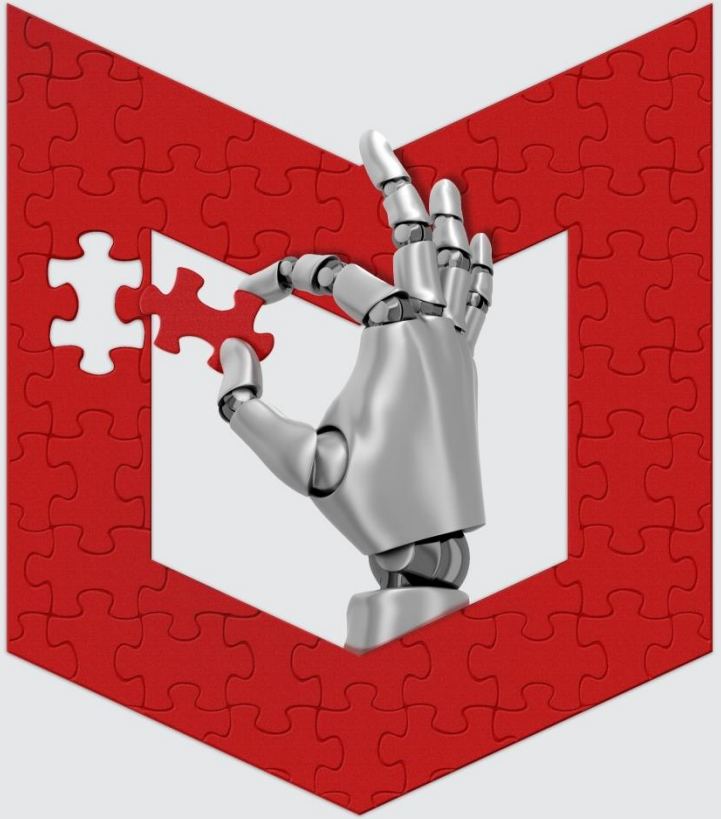
McAfee
Together is power.

Déstabiliser les fauteurs de trouble

Enquête sur la traque des menaces et l'évolution des SOC

www.mcafee.com/fr/solutions/lp/evolution-soc.html



Rapport : *Déstabiliser les fauteurs de trouble, art ou science ?*

Objectif de recherche

Déterminer les meilleures pratiques, actuelles et à venir, en matière de traque des menaces en fonction du degré de maturité de l'entreprise.

- *Impact de l'automatisation, de l'intelligence artificielle et de l'apprentissage automatique*
- *Tactiques de traque spécifiques introduites dans les opérations de base des SOC*
- *Rôle du sandboxing*
- *Outils essentiels à la traque des menaces*
- *Rôle de la cyberveille sur les menaces*

Objectif de recherche et spécifications de l'étude

Spécifications de l'étude

- **727 entretiens**
- Données recueillies lors d'entretiens en ligne
- Entretiens menés en mai 2017

Source des échantillons

- Clients McAfee, membres du comité consultative sur les produits de sécurité de McAfee (*Security Product Advisory Council*)
  - ✓ Clients s'exprimant en anglais, partout dans le monde
- Échantillon du marché général
  - ✓ États-Unis, Canada, Royaume-Uni, Allemagne, Australie, Nouvelle-Zélande et Singapour

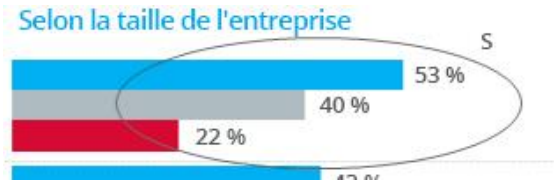
Public cible

- Entreprises employant plus de 1 000 personnes
- Répondants consacrant au moins 20 % de leur temps à la traque des menaces
- Utilisation d'environnements sandbox et de solutions SIEM

Test de signification

- Les différences entre les segments (taille d'entreprise, pays, etc.) présentées dans le rapport sont fondées sur des tests bilatéraux d'un niveau de signification statistique de 95 %.
- Si les résultats d'un segment donné sont sensiblement plus élevés que ceux d'un autre segment, le rapport en fait clairement état.

Exemple



Public visé

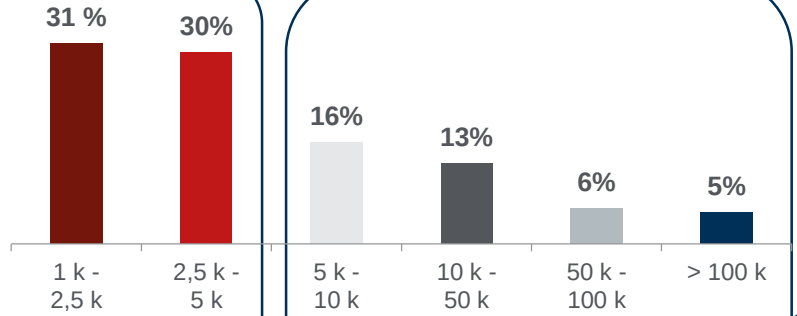
Échantillons de base suffisamment importants pour l'Amérique du Nord, l'Europe et l'Asie

Nombre d'entretiens par région

Pays

USA	CA	UK	AU	DE	IN	NZ	SG	Autre
34 %	8 %	21 %	4 %	19 %	1 %	2 %	10 %	-

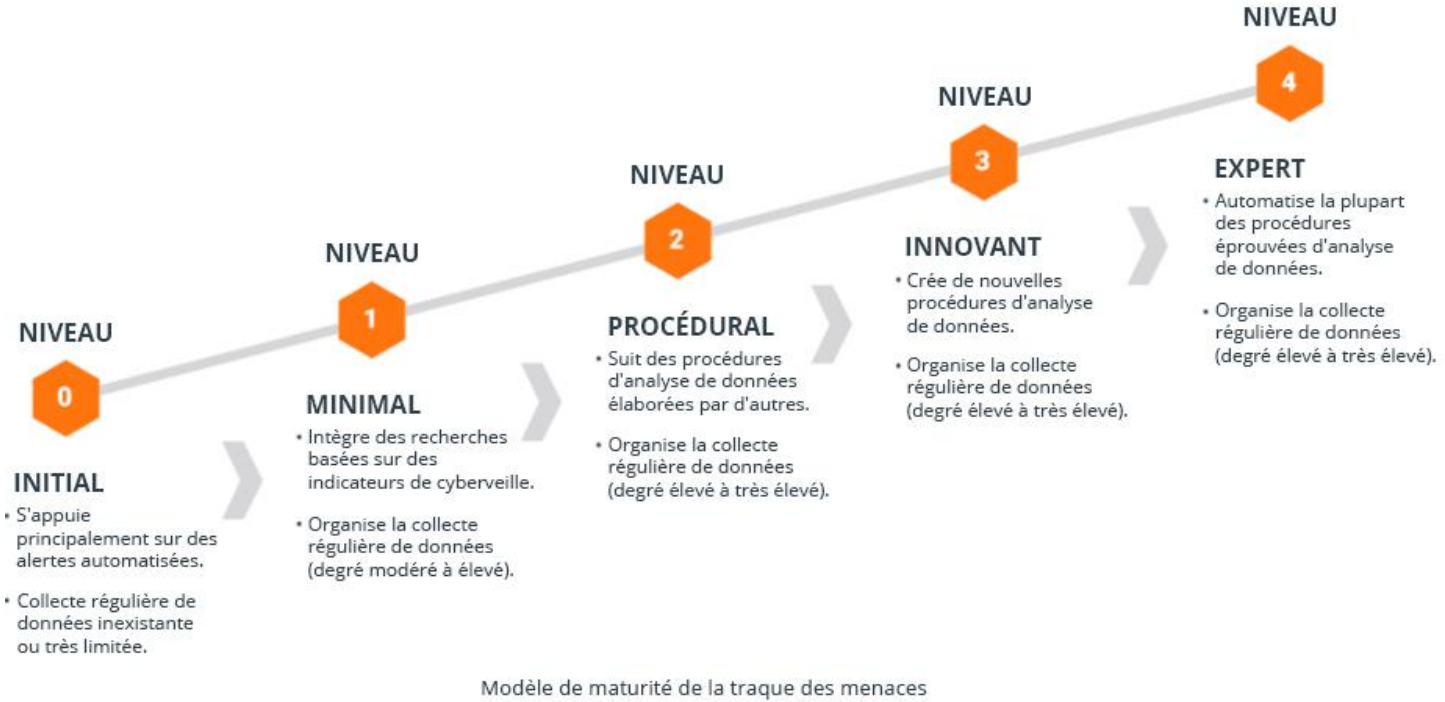
Taille de l'entreprise (nombre de personnes employées)



Moyennes entreprises

Grandes entreprises

Les répondants ont été invités à identifier, parmi 5 niveaux, celui correspondant à leur entreprise

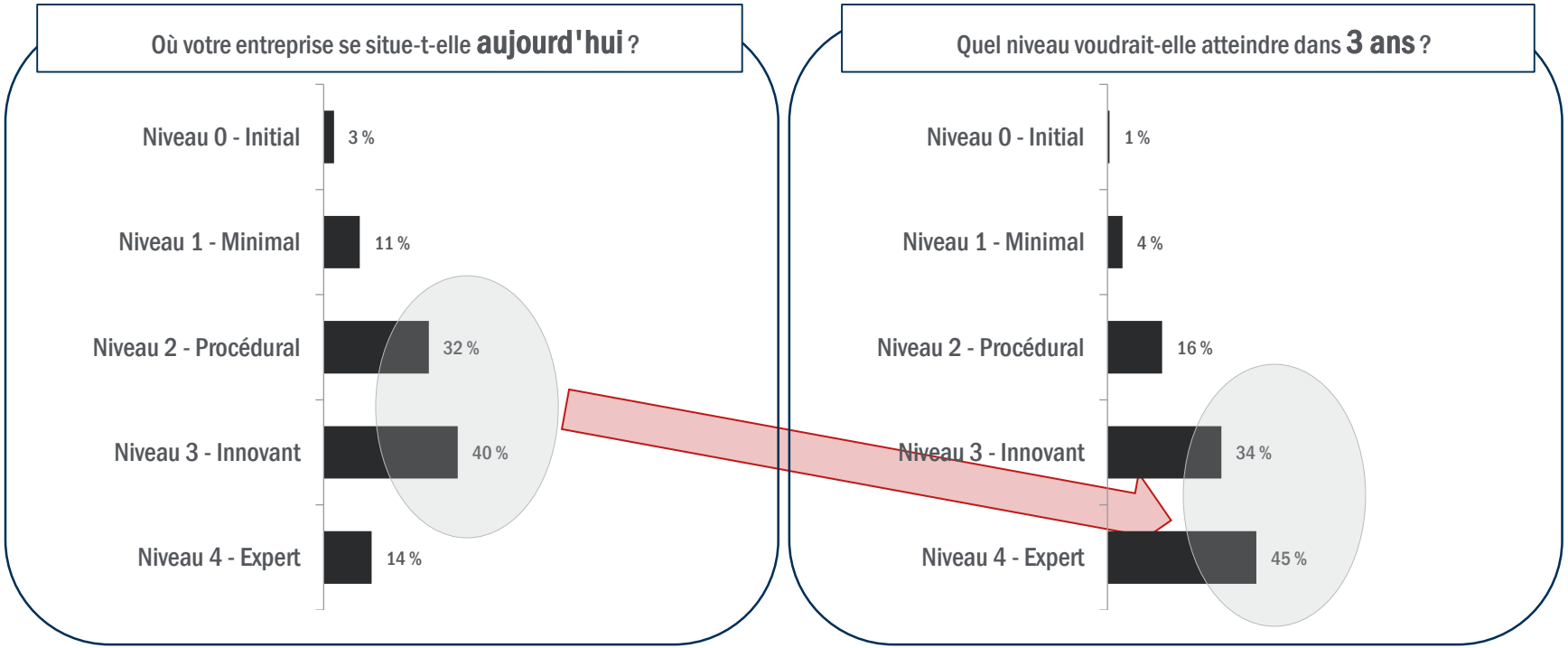


Modèle de maturité de la traque des menaces

Hunting Maturity Model (modèle de maturité de la traque des menaces) développé par David Bianco, expert en technologies de sécurité chez Sqrrl et spécialiste de la traque des menaces

Modèle de maturité – Les sociétés VEULENT s'améliorer

Près de la moitié des entreprises (45 %) interrogées souhaitent atteindre le niveau 4 dans les trois ans.



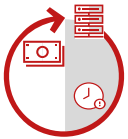
Principales observations : les SOC avancés obtiennent des résultats sensiblement supérieurs

Investigations plus rapides et plus approfondies

71 % les clôturent en moins d'une semaine

4,5 x plus de causes premières identifiées

45 % de valeur en plus grâce à l'utilisation avancée des sandbox

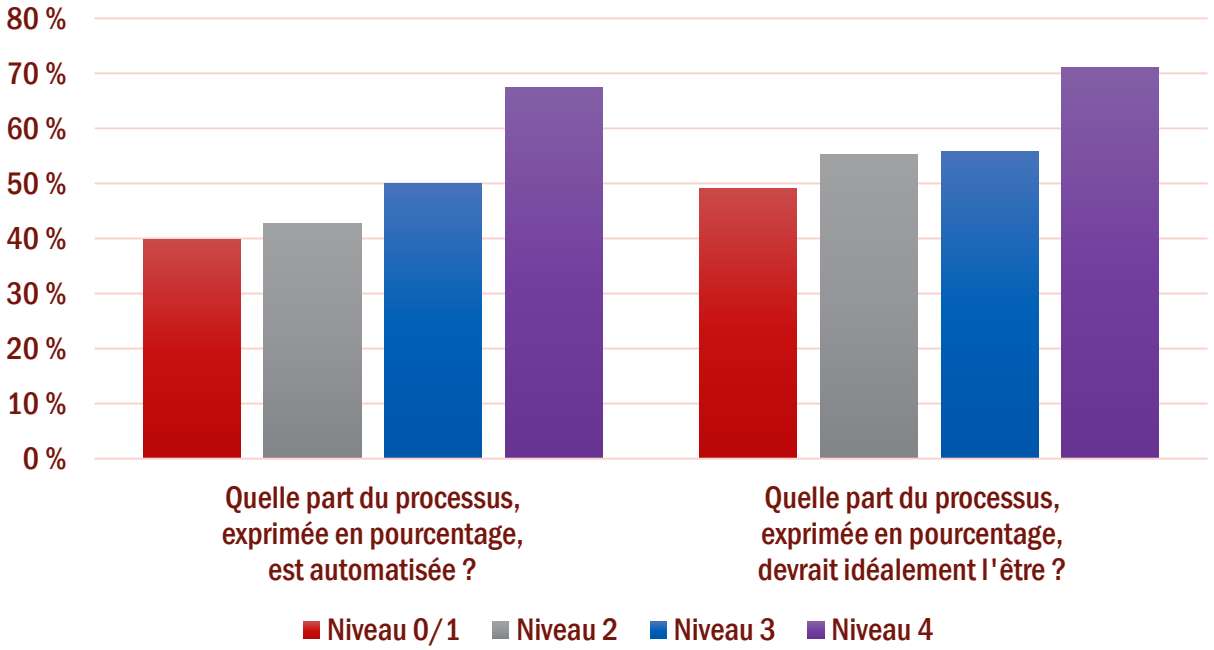


- 71 % des SOC les plus matures parviennent à conclure les investigations des incidents en moins d'une semaine et 37 % clôturent les investigations des menaces en moins de 24 heures.
- Les spécialistes de la traque dans les entreprises plus matures déterminent la cause fondamentale d'une attaque 4,5 fois plus souvent (90 % contre 20 %) que ceux dont l'entreprise se situe plus bas sur la courbe de maturité.
- Les SOC avancés dégagent 45 % de valeur en plus grâce à l'utilisation de sandbox. Ceux-ci leur permettent de gagner du temps, de réduire les coûts, d'améliorer les workflows et de révéler des informations autrement inaccessibles.

Comment les SOC avancés obtiennent-ils de tels résultats?

Identification des solutions optimales et automatisation des processus : duo homme-machine

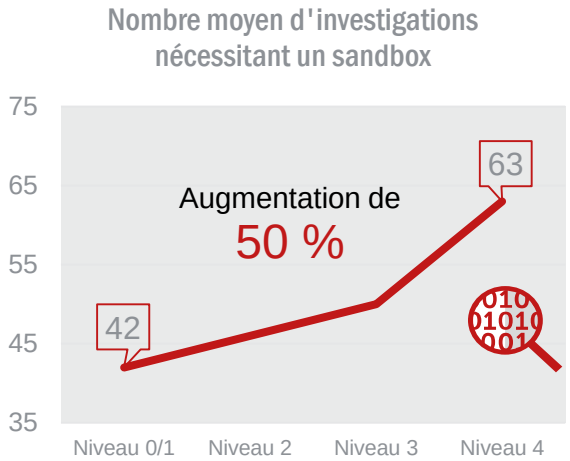
- 68 % estiment pouvoir progresser en **améliorant l'automatisation** et les processus de traque des menaces.
- Les SOC plus matures sont deux fois plus susceptibles de recourir à l'**automatisation.**
- La maturité mène à un meilleur **équilibre** entre une alliance de processus **ad hoc et organisés**. (Il est important de trouver le meilleur moyen d'obtenir des résultats.)



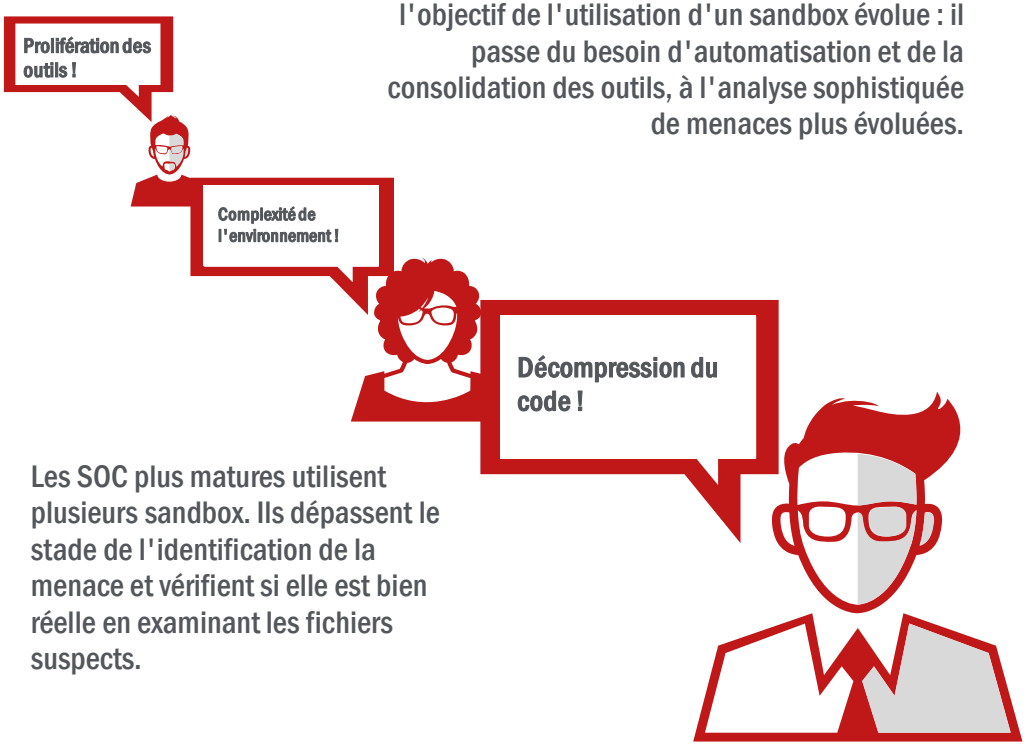
Ils utilisent le sandboxing pour réaliser une analyse plus approfondie

« L'idéal est de pouvoir effectuer des tests de vulnérabilités et d'évincer la menace avant même qu'elle n'apparaisse. Le sandboxing est utile dans un tel scénario. »

Responsable de la traque des menaces interrogé lors des séances qualitatives dans le cadre de l'enquête McAfee sur la traque des menaces, mai 2017



Lorsque le degré de maturité des SOC augmente, l'objectif de l'utilisation d'un sandbox évolue : il passe du besoin d'automatisation et de la consolidation des outils, à l'analyse sophistiquée de menaces plus évoluées.

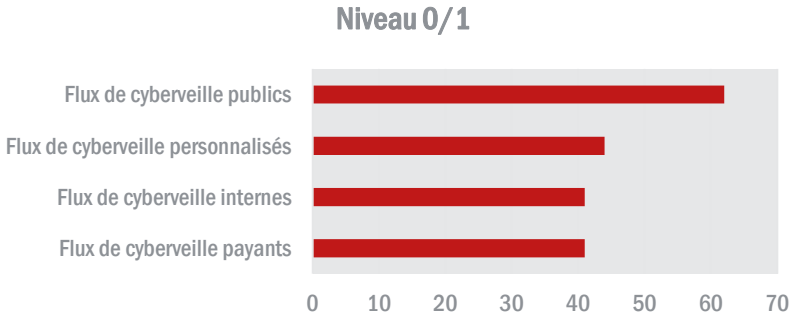


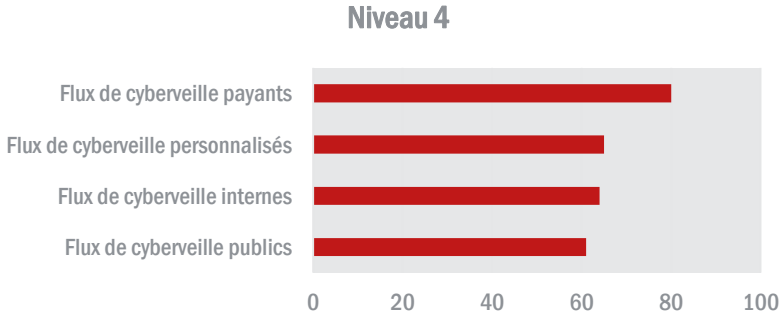
Les SOC plus matures utilisent plusieurs sandbox. Ils dépassent le stade de l'identification de la menace et vérifient si elle est bien réelle en examinant les fichiers suspects.

Ils enrichissement les données de cyberveille par leur collecte auprès de sources pertinentes et sont prêts à payer pour combler leurs lacunes.

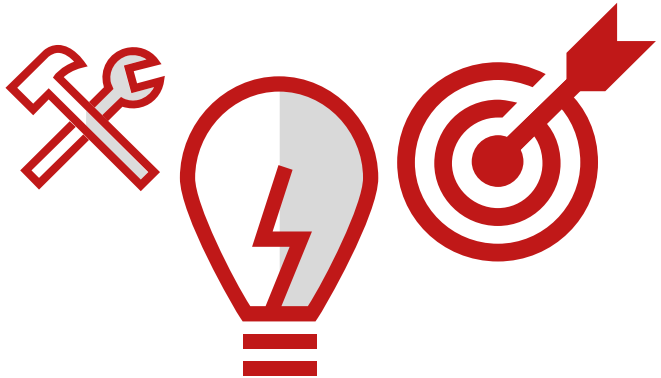
Les SOC de niveaux 0 à 1 s'appuient sur des flux de cyberveille publics **50 %** plus que sur n'importe quel autre type de flux de cyberveille sur les menaces.

En comparaison, les SOC de niveaux 4 sont **2 x** plus enclins à recourir à des flux de cyberveille payants et **50 %** plus susceptibles d'utiliser des flux personnalisés.

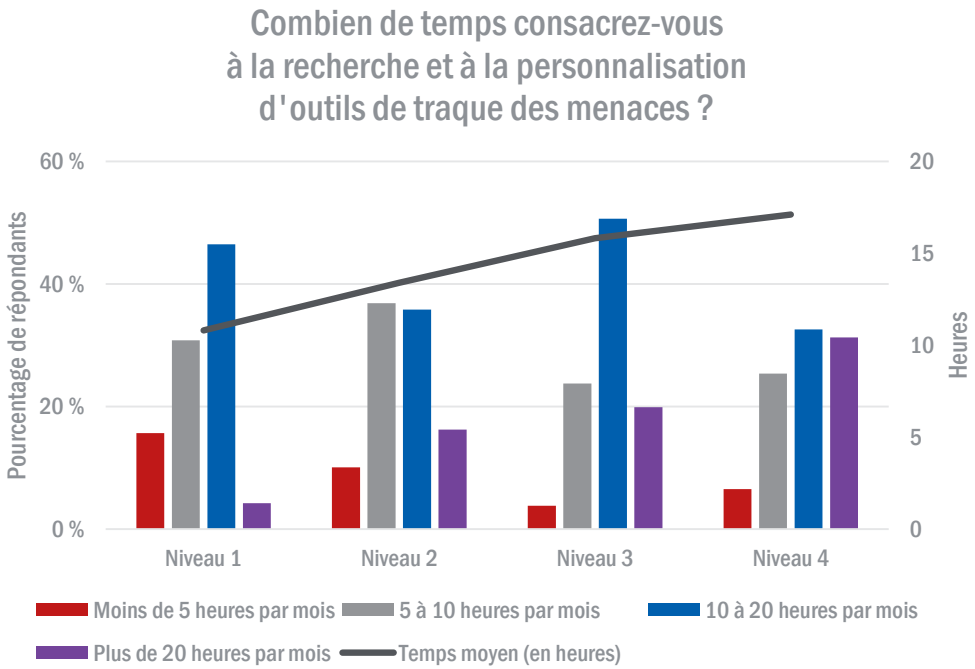




Ils s'appuient davantage sur la personnalisation



Les SOC matures consacrent **70 %** de temps en plus à la personnalisation, en s'appuyant davantage sur des scripts et du code source libre.



Une traque des menaces efficace produit des résultats concrets sans exiger d'efforts acharnés

Clés du succès des entreprises les plus matures :

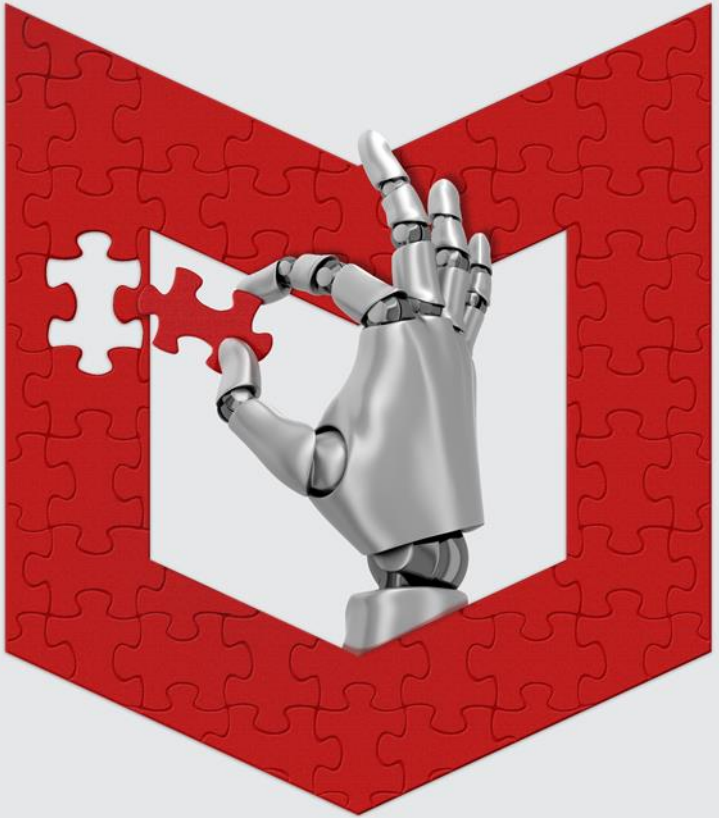
- Identification des processus à automatiser
- Utilisation des outils à disposition pour réaliser une analyse plus approfondie
- Collecte et travail sur une cyberveille pertinente
- Personnalisation et adaptation pour des informations plus riches

Ne vous laissez pas dépasser par l'évolution des SOC

Téléchargez le rapport, les synthèses et les présentations graphiques à l'adresse suivante : www.mcafee.com/fr/solutions/lp/evolution-soc.html

Suivez toute l'actualité en vous abonnant à notre newsletter bimensuelle *McAfee SIEM Insider* : https://www.mcafee.com/fr/products/lp/siem-newsletter-signup.aspx

Écoutez l'analyse de Peter Stephenson (spécialiste en technologies, SC Magazine) et de Michael Leland (McAfee) sur la Recherche de contexte dans le cadre de la traque de menaces avancées (Finding Context in Advanced Threat Hunting). Inscrivez-vous au webcast à l'adresse suivante : https://www.mcafee.com/fr/events/webinars.aspx




McAfee™
Together is power.