Les secrets d'une traque des menaces efficace

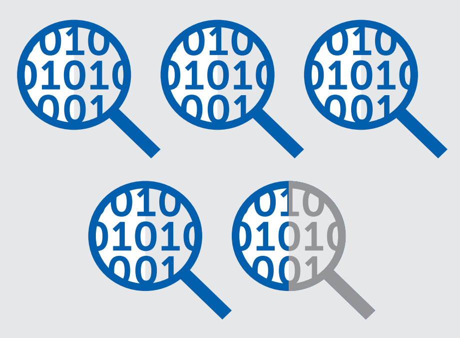
Les équipes de traque des menaces les plus matures ont d'importants atouts

37 %

Investigations performantes

37 % conclues en moins de 24 h

4,5x



Identification des causes premières

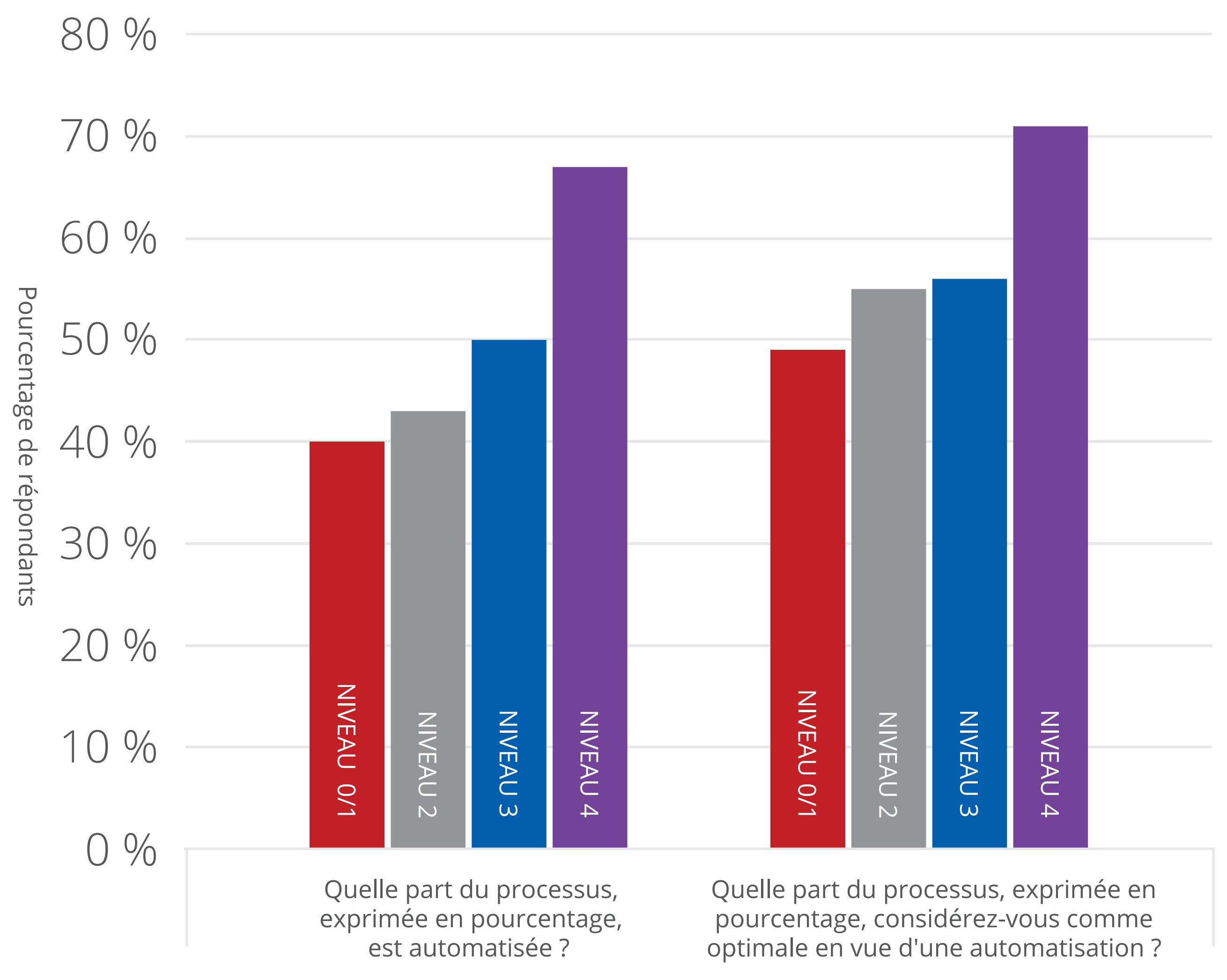
4,5x plus susceptibles de retracer la source

45 %

Amélioration des workflows

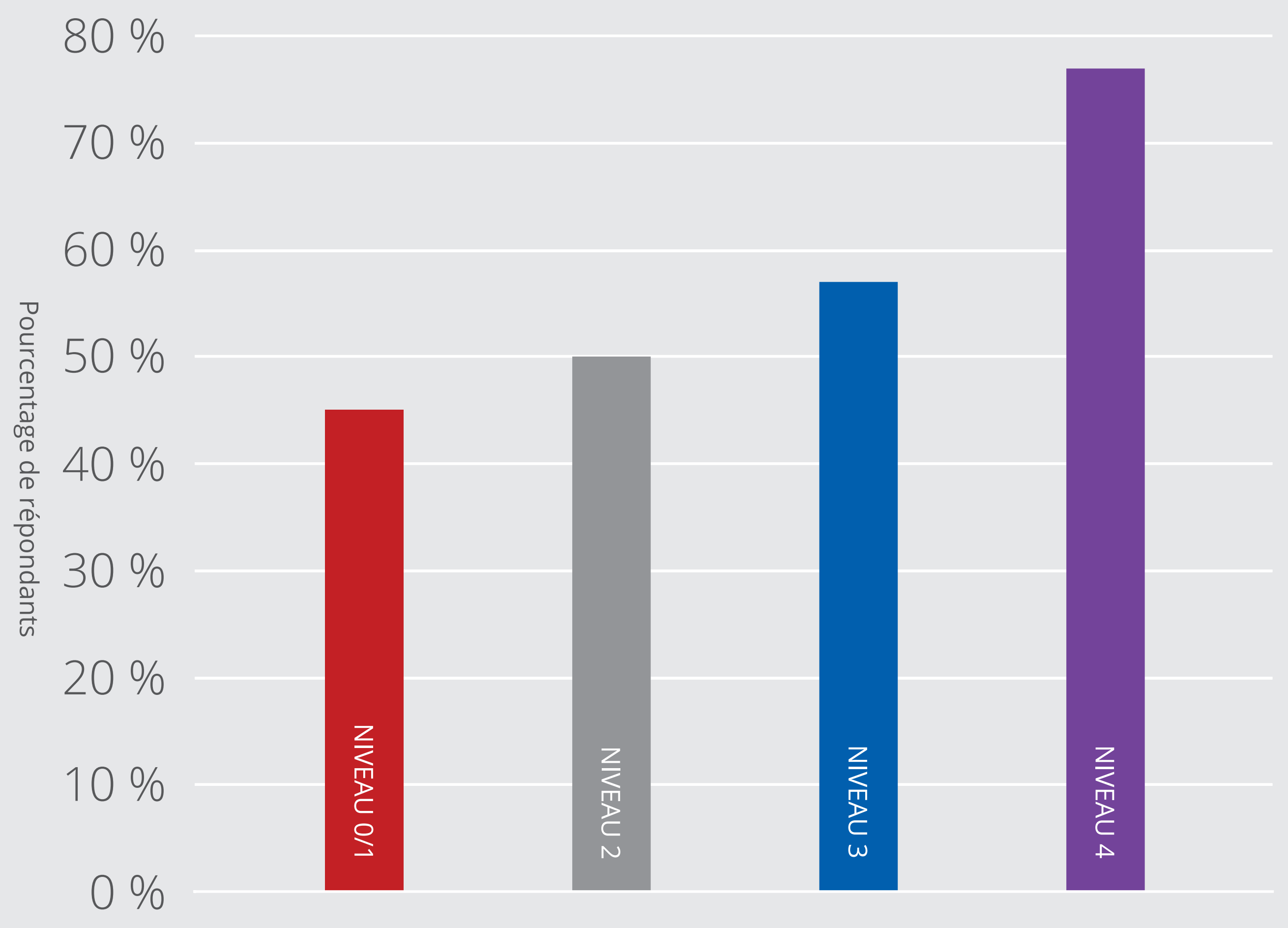
45 % de valeur en plus grâce à l'utilisation d'un sandbox

75 % automatisent l'investigation des attaques : leurs experts peuvent consacrer 50 % de temps en plus aux opérations de traque



Les équipes les plus matures sont 2x plus susceptibles d'automatiser certaines étapes de leur processus, en particulier l'analyse antimalware et l'analyse en temps réel des terminaux.

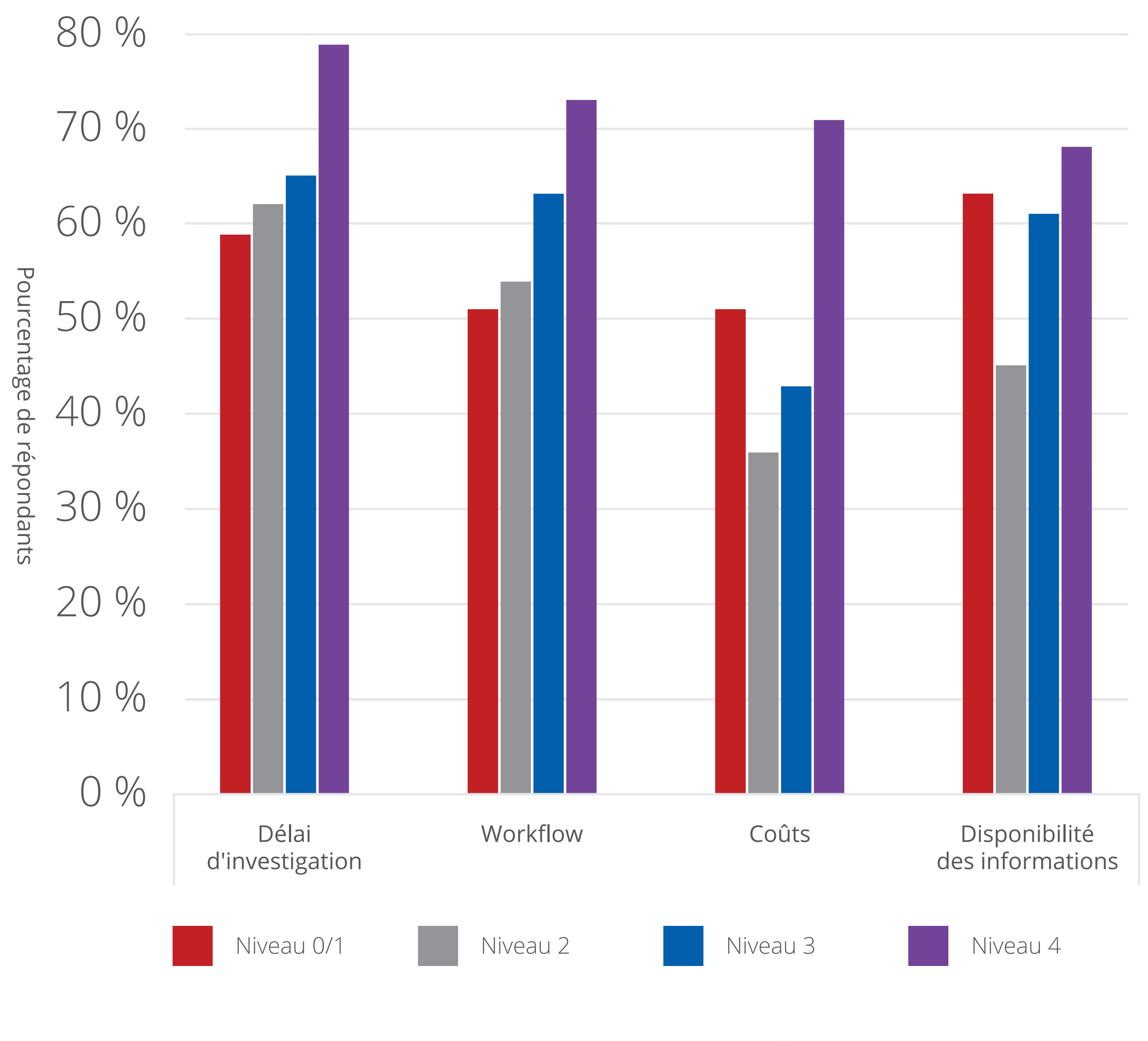
4 sur 5 extraient directement les indicateurs de compromission vers leur SIEM pour une analyse automatisée



La mise en corrélation des indicateurs de compromission permet d'identifier les flux de cyberveille pertinents, de surveiller les événements récurrents et d'en examiner l'historique, mais aussi de filtrer les données pour se concentrer sur les indices.

Les meilleurs SOC utilisent le sandboxing pour réduire les coûts et les efforts, gagner du temps et éliminer les « angles morts »

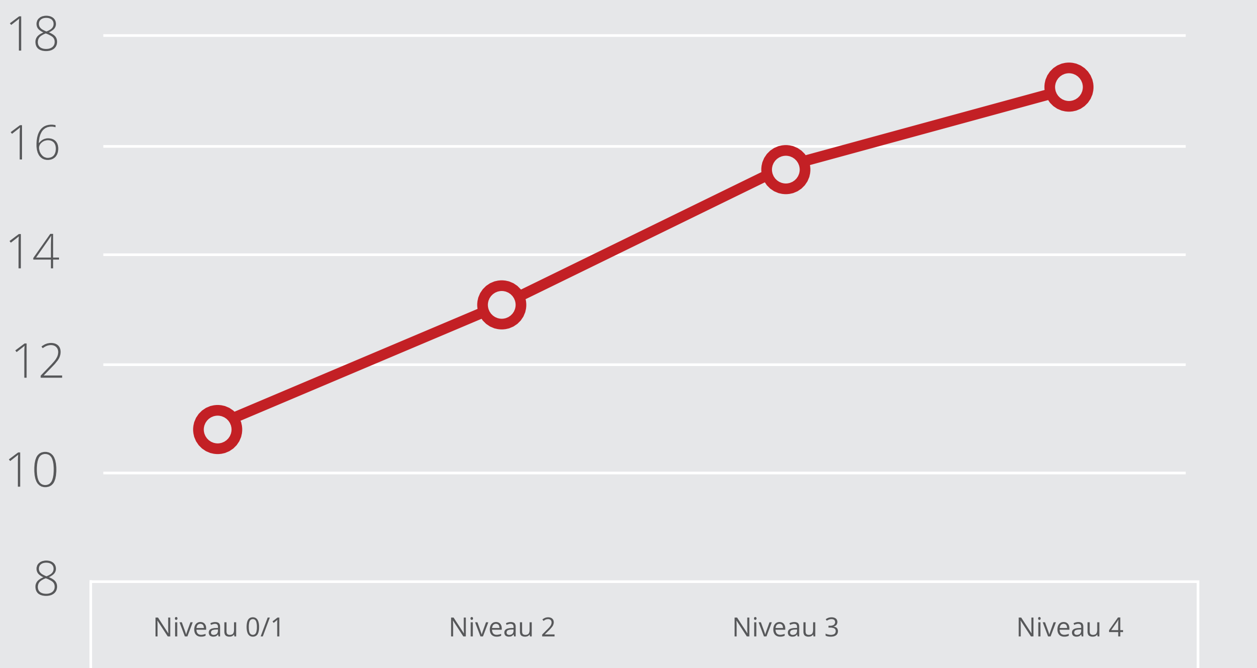
Quelles améliorations importantes permet l'utilisation d'un sandbox dans le cadre des investigations ?



Comment s'expliquent les valeurs supérieures ? Les SOC matures recourent davantage à des fonctions sophistiquées, notamment l'investigation détaillée des menaces et des actions automatisées si la menace est avérée.

Les leaders font preuve d'inventivité

Nombre moyen d'heures imparties à la personnalisation des outils de traque



Les SOC matures prennent l'avantage parce qu'ils consacrent 70 % de temps en plus à la création d'outils et de techniques en s'appuyant sur des scripts et du code source libre.

Le moment est venu de suivre l'exemple des experts de la traque des menaces. Découvrez leurs indices de mesure, tactiques et stratégies dans ce rapport :

RAPPORT

McAfee
Together is power.

Déstabiliser les fauteurs de troubles, art ou science ?

Comprendre le rôle des spécialistes de la traque des menaces et l'importance de l'évolution continue du SOC en matière de cybersécurité

Déstabiliser les fauteurs de trouble, art ou science ?

Pour obtenir le rapport complet :
www.mcafee.com/soc-evolution.

McAfee™
Together is power.

3454_0717_info-disrupting-disruptors-art-science