Évaluation MITRE ATT&CK

IBM Security ReaQta propose les meilleures fonctionnalités dans sa catégorie

En bref

Privilégiez la continuité des opérations tout en libérant votre équipe de sécurité de l'analyse manuelle des cybermenaces.

Réduisez les alarmes incessantes et simplifiez votre cybersécurité en générant le minimum d'alertes de menaces.

Bénéficiez d'une visibilité complète sur vos points de terminaison pour répondre rapidement à chaque étape

À propos du rapport

ReaQta, une société IBM, a terminé avec succès l'évaluation MITRE ATT&CK. Ce rapport montre que la solution ReaQta fournit une couverture complète contre les attaques sophistiquées presque sans aucune intervention humaine, tout en produisant des alertes de qualité supérieure.

Qu'est-ce qu'une évaluation MITRE ATT&CK ?

MITRE ATT&CK définit un ensemble d'étapes au cours d'une cyberattaque et évalue les solutions sur leur capacité à détecter les menaces. Chacune des étapes répertoriées représente une « tactique » dans la chaîne cybercriminelle :

- Accès initial
- Exécution
- Persistance
- Escalade de privilèges
- Contournement de la défense
- Accès aux données d'identification
- Reconnaissance
- Mouvement latéral
- Collecte
- Exfiltration
- Commandement et contrôle

Comment l'évaluation MITRE aide les organisations

L'évaluation n'a pas pour but de noter ou de classer les solutions, mais d'aider les organisations à identifier la solution la plus adaptée à leurs besoins en sécurité. Les organisations doivent savoir que l'évaluation se déroule dans des environnements isolés et présente des limites. Il arrive que certaines fonctions d'une solution soient désactivées, parce qu'elles ne sont pas compatibles avec l'infrastructure du laboratoire, comme dans le cas de ReaQta NanoOS, où l'hyperviseur en direct utilisé pour détecter les comportements malveillants de haut niveau ne pouvait pas être utilisé. Néanmoins, la plateforme a bien réagi, malgré l'absence de composant principal.

MITRE dispose d'un ensemble de techniques identifiées, chacune d'entre elles appartenant à un groupe tactique basé sur l'acteur de la menace sélectionné pour l'évaluation. MITRE a choisi APT29 pour ce cycle d' évaluation.

Compromettre

Collecte et contournement

Reconnaissance

Étendre l'accès

Exfiltration

Nettoyage

Privilégiez la continuité des opérations, tout en libérant votre équipe de sécurité de l'analyse manuelle des cybermenaces.

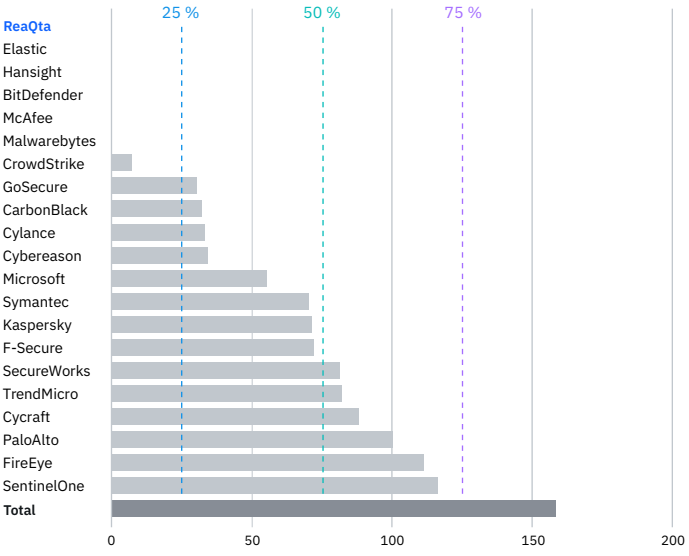
Avant de commencer l'évaluation, ReaQta a choisi de participer sans fournisseur de services de sécurité gérés (MSSP), c'est-à-dire sans aucune interaction humaine pendant l'attaque. MITRE est un cadre d'évaluation des technologies, et il semblait peu approprié d'impliquer des personnes. De plus, la contribution des détections MSSP biaise fortement l'évaluation. L'équipe du centre des opérations de sécurité (SOC) sait qu'une attaque est en cours et exactement où et comment.

L'approche MSSP n'aurait pas permis aux clients de ReaQta de disposer d'une évaluation juste de la technologie. MITRE a tenu compte des commentaires, et à partir de la troisième phase, toutes les entreprises seront évaluées sans intervention humaine.

Les MSSP apportent une grande valeur ajoutée, et les clients devraient être libres de choisir entre les MSSP et les déploiements autonomes.

Comme le montre le graphique ci-dessous, le nombre de détections effectuées par des personnes a un impact énorme sur les détections générées. Dans plusieurs cas, plus de 50 % des détections, et jusqu'à 73 %, ont été créées manuellement. Seules 6 entreprises ont décidé de participer sans impliquer de personnes dans la boucle.

Détections MSSP (générées manuellement)



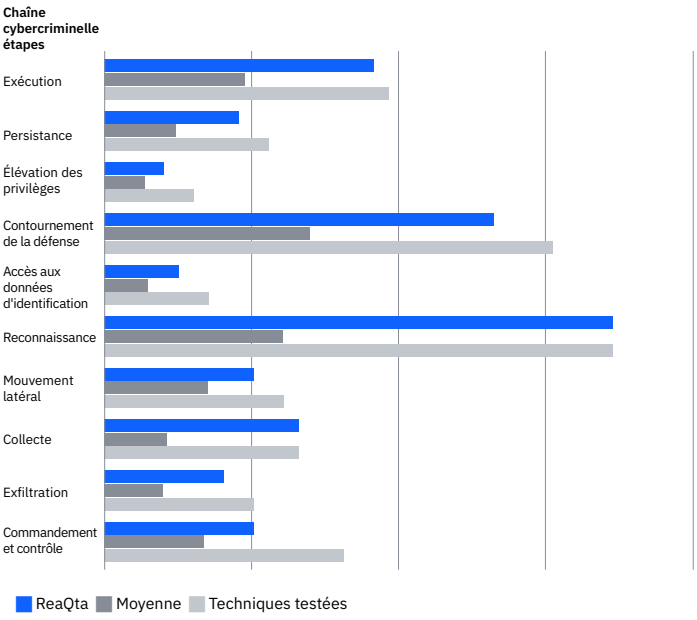
Détections manuelles généré par chaque fournisseur

Évaluation MITRE Phase 2—APT29

Les fournisseurs ont été testés sur leur capacité à détecter les tactiques et techniques utilisées par APT29 (également appelé The Dukes, Cozy Bear et CozyDuke), un adversaire sophistiqué de type État-nation connu pour son approche furtive. APT29 est largement connu pour être à l'origine d'attaques notables : le Pentagone en 2015, le Democratic National Committee en 2016, et les gouvernements norvégien et néerlandais en 2017.

Le changement par rapport à la phase précédente était important : APT3 (Phase 1) est un acteur de la menace bruyant, qui adopte divers outils beaucoup moins discret. APT29, en revanche, est extrêmement furtif, opérant avec discrétion et s'appuyant fortement sur les LOLBins et les logiciels malveillants sans fichier.

Couverture de détection des techniques (automatisée)



Couverture de la détection automatisée ReaQta par rapport à la moyenne

Résultats de l'évaluation ReaQta

L'attaque s'est déroulée sur deux jours au cours desquels les attaquants ont progressivement pénétré dans le réseau après avoir obtenu un accès initial. La grande majorité des opérations ont été réalisées à l'aide de Microsoft PowerShell, par opposition aux outils personnalisés et aux logiciels malveillants, à des fins des fins de discrétion. L'objectif de l'évaluation est de montrer comment les solutions testées répondent à l'attaque et quel type de visibilité est fourni tout au long de la chaîne cybercriminelle.

Comme le montre le résumé des résultats de l'évaluation, ReaQta a fourni une visibilité complète sur l'ensemble de la chaîne cybercriminelle. ReaQta a détecté 90 % des tactiques et techniques testées, prouvant ainsi sa capacité à répondre aux menaces et à y remédier à chaque étape de l'attaque.

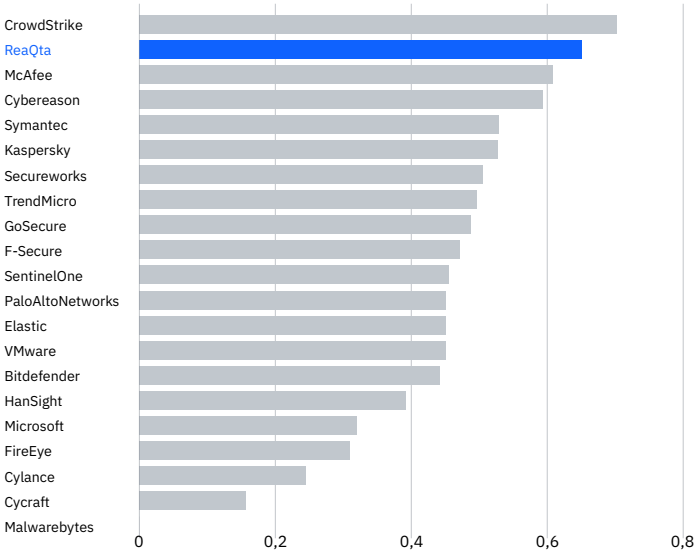
ReaQta affiche l'un des meilleurs taux d'exploitabilité au monde, même par rapport aux fournisseurs qui s'appuient sur les détections manuelles des MSSP.

Réduisez les alarmes incessantes et simplifiez votre cybersécurité en générant le nombre minimum d'alertes de menaces nécessaires.

La plateforme a détecté et généré des alertes dès les étapes d'exécution, de persistance, d'escalade de privilèges et de contournement de la défense, permettant à l'équipe de sécurité de suivre APT29 et ses actions. Les alertes de la plateforme étaient cohérentes au cours des dernières étapes de la chaîne cybercriminelle : mouvement latéral, collecte, exfiltration et commandement et contrôle, ce qui montre la capacité de ReaQta à réagir et à limiter les dommages, même au cours des dernières étapes d'une cyberattaque.

Le taux d'exploitabilité a mis en évidence la capacité de la plateforme à réduire le bruit en diminuant le nombre d'alertes générées. Elle a capturé toutes les tactiques et techniques en quelques alertes corrélées, par rapport à une alerte par tactique et technique, ce qui représenterait un nombre ingérable d'alertes à examiner et à traiter par les équipes du SOC.

Exploitabilité des alertes

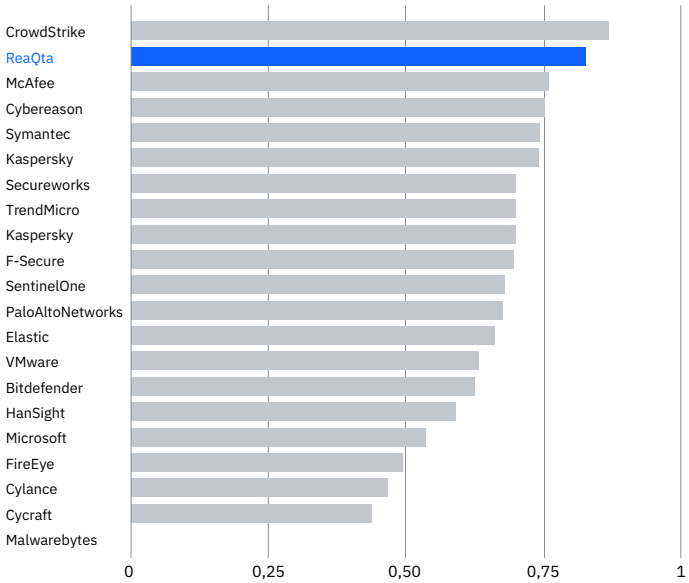


Qualité des alertes (les données incluent les détections manuelles pour les fournisseurs s'appuyant sur des MSSP)

Là aussi, ReaQta fournit des alertes de haute qualité sans intervention humaine, alors que le premier et le troisième fournisseurs ont eu recours à l'analyse manuelle pendant l'évaluation.

Le niveau de visibilité fourni par ReaQta rend nécessaire de filtrer les données, de les corréler et de générer le plus petit nombre possible d'alertes, chacune contenant la plus grande quantité d'informations connexes. C'est le rôle des moteurs d'IA de ReaQta : collecter, corréler et synthétiser la télémétrie. La qualité des alertes est également confirmée par l'analyse de Forrester dans le graphique ci-dessous.

Qualité des alertes



Qualité des alertes (les données incluent les détections manuelles pour les fournisseurs s'appuyant sur des MSSP)

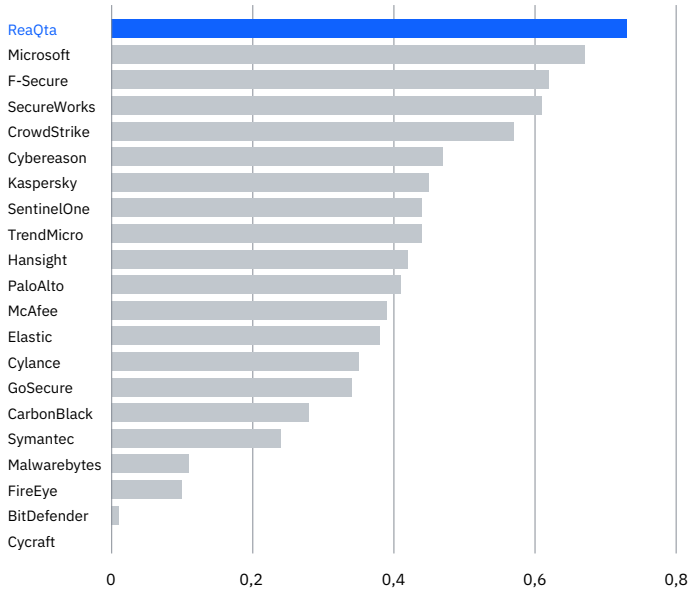
« L'exploitabilité est le produit de l'efficacité et de la qualité des alertes [...] l'efficacité des alertes (pas trop nombreuses) et la qualité des alertes (dans quelle mesure elles aident à comprendre la situation) sont toutes deux liées et essentielles pour comprendre dans quelle mesure une alerte particulière sera exploitable. »

Forrester[2]

Fournir des alertes complètes et de haute fidélité est le critère qui distingue une bonne plateforme des simples générateurs de bruit.

Le graphique ci-dessous montre le comportement ReaQta par rapport aux autres solutions lorsque les détections manuelles sont supprimées. Chaque barre représente la quantité d'informations liées à l'incident capturées dans le cadre de chaque alerte générée. Les moteurs de ReaQta ont capturé la plus grande quantité d'informations, ce qui se traduit par une réduction considérable de la charge de travail dans les environnements réels.

Couverture des attaques par alerte générée (rapport signal/bruit)



Pourcentage de couverture d'attaque par alerte

ReaQta n'a généré que 25 alertes et a collecté correctement toutes les informations nécessaires pour traquer les attaquants dans chacune d'entre elles, au lieu d'en créer 158, une par technique testée.

La capacité à fournir un flux unifié pour la résolution des incidents est essentielle pour réduire les alertes incessantes.

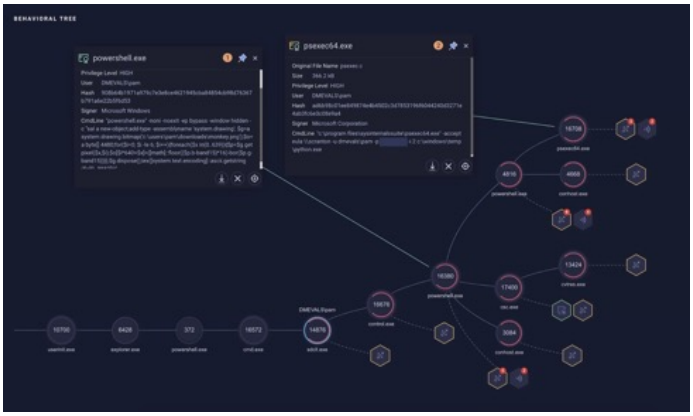
ReaQta a corrélé le scénario lors de l'évaluation MITRE. Ainsi, les analystes ont pu comprendre et étudier facilement un attaquant actif, sans être distraits par des centaines d'alertes générées sans relation directe avec l'incident d'origine. Cela aurait été beaucoup plus difficile à gérer lors d'une analyse réelle.

L'approche ReaQta a permis de réduire de 85 % les alertes incessantes en préservant une visibilité totale sur l'ensemble de l'attaque. ReaQta est spécialement conçu pour générer le nombre minimal d'alertes par incident, facilitant ainsi une analyse fluide et ininterrompue. Grâce à la possibilité de tout conserver dans une seule et même vue, les analystes peuvent réagir plus rapidement, sans qu'il soit nécessaire de passer d'une vue à une autre pour comprendre complètement les événements.

Bénéficier d'une visibilité complète de vos points de terminaison pour répondre rapidement à chaque étape.

La plateforme a pu maintenir la corrélation entre les actions à toutes les étapes de la chaîne cybercriminelle ATT&CK. La corrélation automatique des événements accélère la reconstitution des différentes actions exécutées par les attaquants et, finalement, réduit le temps de réponse en cas d'attaque réelle.

Arbre comportemental



Scénario corrélé ReaQta lors de l' évaluation MITRE

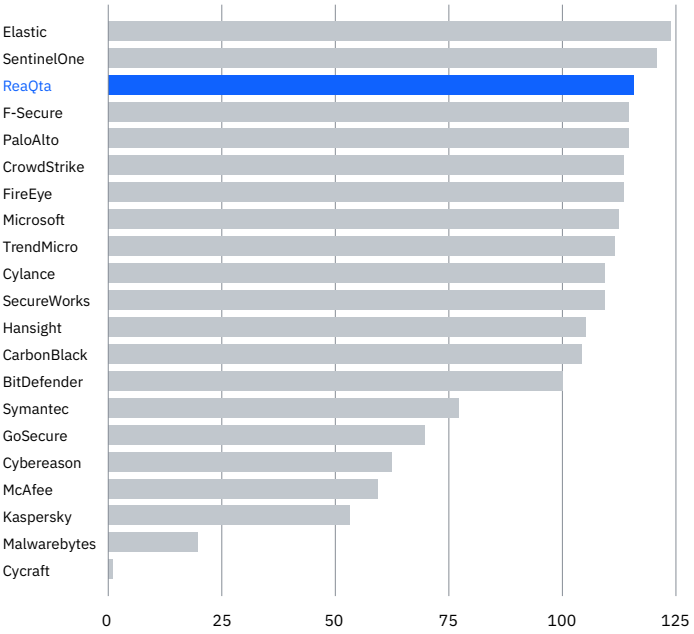
Pour fournir un exemple lié à l'évaluation, le graphique ci-dessus montre comment une étape entière de l'attaque a été capturée dans une seule alerte. ReaQta a corrélé toutes les informations dans un scénario facilement compréhensible, fournissant ainsi à une équipe SOC toutes les informations pour un triage rapide. Aucune interaction humaine n'a été nécessaire, et l'attaque a été clairement expliquée, et son risque évalué, sans nécessiter aucune activité manuelle.

En examinant de plus près la détection des tactiques et techniques d'APT29, ReaQta a fourni une visibilité depuis les premières étapes de la chaîne cybercriminelle jusqu'aux étapes plus sophistiquées qui sont souvent plus difficiles à détecter. Ce qui est remarquable ici, c'est la capacité de la plateforme à détecter uniformément les menaces à chaque étape, offrant ainsi des possibilités de réponse et de remédiation pour chacune d'entre elles.

ReaQta a montré l'une des meilleures télémétries, associée à un impressionnant moteur IA capable de condenser les informations et d'évaluer les risques. Il s'avérera un outil puissant dans un SOC ou dans une équipe qui souhaite consacrer du temps à la chasse aux menaces au lieu de gérer constamment des alertes.

ReaQta a montré l'une des meilleures télémétries.

Télémétrie



Quantité de télémétrie fournie par ReaQta

Conclusion

La plateforme optimisée par l'IA de ReaQta dote les équipes de sécurité de fonctionnalités avancées de détection et de réponse rapide, réduisant ainsi l'intervention humaine, simplifiant l'ensemble du processus de cybersécurité et favorisant la continuité des opérations, qu'elle que soit la taille de l'organisation.

Cette évaluation a validé l'approche de ReaQta dans le domaine de la détection des acteurs de menaces sophistiquées. ReaQta continuera à participer à des tests indépendants de tiers à l'avenir.

ReaQta apprécie et loue le travail de MITRE qui aide les organisations à prendre des décisions éclairées grâce à ces évaluations.

Pour plus d'informations, rendez-vous sur :
ibm.com/products/reaqta

Compagn ie IBM France
17 avenue de l’Europe
92275 Bois-Colombes Cedex

Produit aux États-Unis d'Amérique
1er mars 2022

1 MITRE ATT&CK evaluation, The MITRE Corporation and MITRE Engenuity, 2020.
2 Further Down the Rabbit Hole With MITRE’s ATT&CK Eval Data, Forrester blog, 4 May 2020.