Avaliação MITRE ATT&CK

O IBM Security ReaQta apresenta os melhores recursos da categoria

Destaques

Promova a continuidade de negócios enquanto libera sua equipe de segurança da análise manual de ameaças cibernéticas

Reduza a fadiga de alertas e simplifique sua segurança cibernética gerando a quantidade mínima de alertas de ameaças

Tenha visibilidade completa de seus terminais para permitir respostas rápidas em todas as etapas

Sobre o relatório

A ReaQta, uma empresa IBM, concluiu a avaliação MITRE ATT&CK com sucesso. Este relatório mostra que a ReaQta oferece cobertura completa contra ataques sofisticados, produzindo alertas de altíssima qualidade praticamente sem nenhuma interação humana.

O que é uma avaliação MITRE ATT&CK?

A MITRE ATT&CK define um conjunto de etapas durante um ciberataque e avalia as soluções em sua capacidade de detectar ameaças. Cada uma das etapas listadas representa uma “tática” ao longo da kill-chain:

- Acesso inicial
- Execução
- Persistência
- Escalada de privilégio
- Evasão de defesas
- Acesso de credenciais
- Descoberta
- Movimento lateral
- Coleta
- Exfiltração
- Comando e controle

Como a avaliação MITRE ajuda as organizações

A avaliação de segurança não pontua ou classifica soluções e tem o propósito de ajudar organizações a identificar a solução mais adequada para seus desafios específicos de segurança. No entanto, as organizações precisam observar que a avaliação acontece em ambientes isolados e possui limitações. Existem momentos em que certos recursos de uma solução são desativados, pois não oferecem suporte a uma determinada infraestrutura do laboratório, como no caso do ReaQta NanoOS, em que não foi possível utilizar o hypervisor em tempo real usado para detectar comportamentos maliciosos de grau elevado. Ainda assim a plataforma teve um bom desempenho, mesmo sem o seu componente principal.

A MITRE possui um conjunto identificado de técnicas, sendo que cada qual pertence a um grupo de táticas baseado no agente de ameaça selecionado para a avaliação. A MITRE escolheu o APT29 para esta rodada de avaliação.

Concessão

Coleta e evasão

Reconhecimento

Expansão de acesso

Exfiltração

Limpeza

Promova a continuidade de negócios enquanto libera sua equipe de segurança da análise manual de ameaças cibernéticas

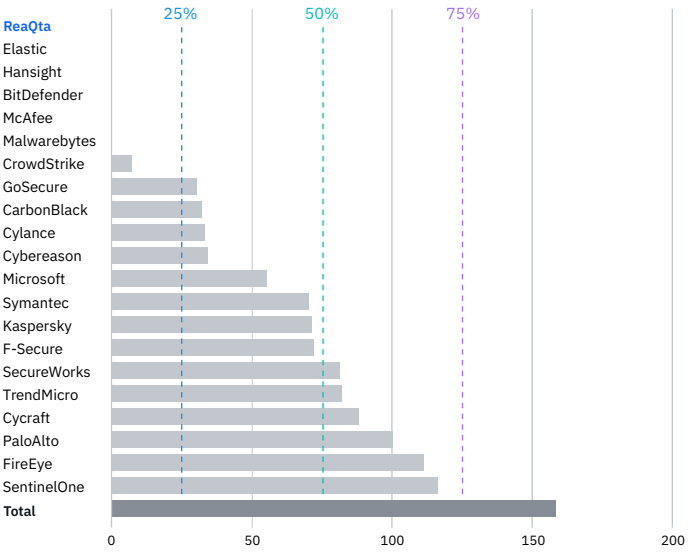
Antes de iniciar a avaliação, a ReaQta decidiu participar sem um provedor de serviço de segurança gerenciado (MSSP), isto é, sem nenhuma interação humana durante o ataque. MITRE é um modelo de avaliação de tecnologia e introduzir intervenção humana na equação seria pouco honesto de nossa parte. Além disso, a contribuição das detecções de MSSP influencia a avaliação excessivamente. A equipe de operações segurança (SOC) sabe que um ataque está acontecendo, exatamente onde e como.

A abordagem MSSP não teria proporcionado aos clientes da ReaQta uma avaliação justa da tecnologia. A MITRE tem sido muito receptiva ao feedback e, a partir da Rodada 3, todas as empresas serão avaliadas sem a participação de humanos.

No entanto, MSSPs agregam bastante valor e os clientes devem ser livres para escolher entre implementações por MSSP ou independentes.

Conforme mostrado no gráfico abaixo, o número de detecções realizadas por humanos teve um enorme impacto nas detecções geradas. Em vários casos, mais de 50% das detecções, chegando a 73%, foram criadas manualmente. Apenas seis empresas decidiram eliminar a participação de humanos.

Detecções MSSP (geradas manualmente)



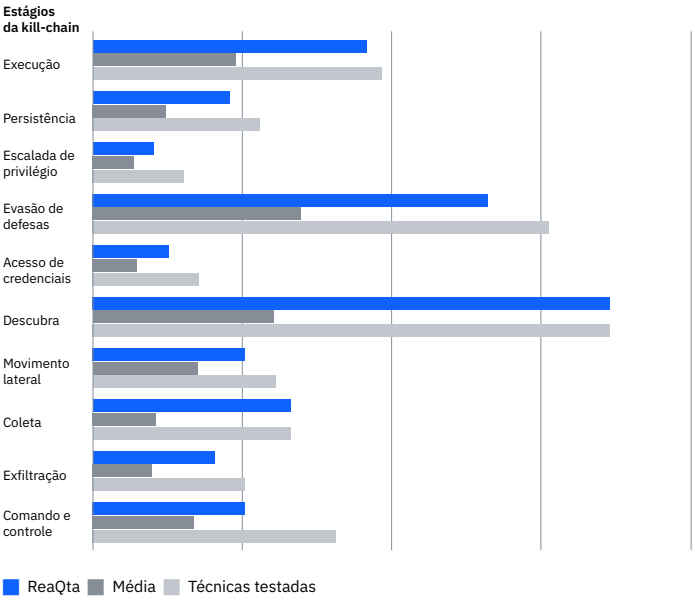
Detecções manuais geradas por cada fornecedor

Avaliação MITRE Rodada 2—APT29

Os fornecedores foram testados de acordo com suas capacidades de detectar as táticas e técnicas utilizadas pelo APT29 (também conhecido como The Dukes, Cozy Bear e CozyDuke), um adversário conhecido de diversos estados nacionais por sua abordagem furtiva. O APT29 é amplamente conhecido como responsável por ataques notáveis: Pentágono em 2015, o Comitê Nacional Democrata dos EUA em 2016 e os governos norueguês e holandês em 2017.

A mudança em relação à rodada anterior é relevante: APT3 (Rodada 1) é um agente de ameaça barulhento, que adota diversas ferramentas sem muita preocupação em não chamar atenção. APT29, por outro lado, é extremamente furtivo, agindo de maneira extremamente discreta e com alta taxa de uso de LOLBins e fileless malware.

Cobertura da detecção de técnicas (automatizada)



Cobertura de detecção automatizada da ReaQta em comparação com a média

Resultados da avaliação da ReaQta

O ataque se desenrolou ao longo de dois dias, nos quais os invasores se aprofundaram gradualmente na rede após conseguir o acesso inicial. A grande maioria das operações foram realizadas por meio do Microsoft PowerShell em vez de ferramentas customizadas e malware, a fim de manter um perfil discreto para evitar detecção. O objetivo da avaliação é mostrar como soluções testadas respondem ao ataque e que tipo de visibilidade é fornecida ao longo de toda a kill chain.

Como fica evidente no resumo dos resultados da avaliação, a ReaQta forneceu visibilidade completa em toda a kill chain. A ReaQta detectou 90% das táticas e técnicas testadas, comprovando sua capacidade de responder e corrigir ameaças em todas as fases do ataque.

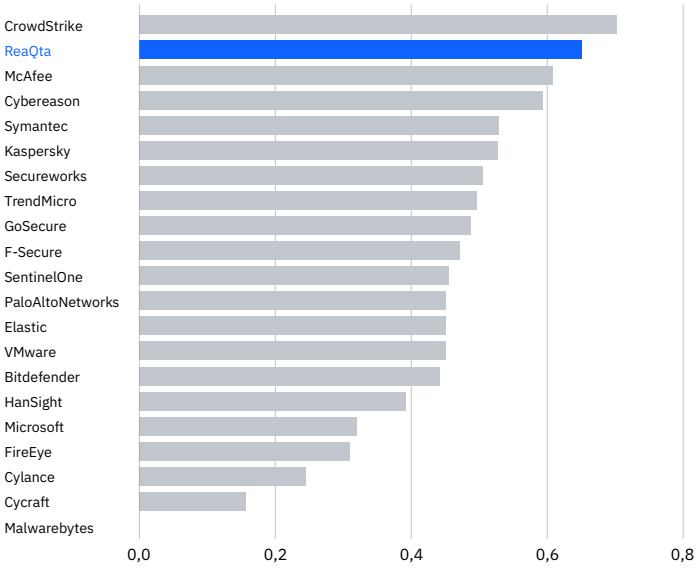
A ReaQta possui uma das maiores taxas acionáveis do mundo, mesmo quando comparada com fornecedores que dependem de detecções manuais por MSSPs.

Reduza a fadiga de alertas e simplifique sua segurança cibernética reduzindo o número de alertas de ameaças

A plataforma detectou e gerou alertas assim que iniciou os estágios de execução, persistência, escalada de privilégio e evasão de defesas, permitindo que a equipe de segurança acompanhasse o APT29 e todas as suas ações. Os alertas da plataforma foram consistente durante os últimos estágios da kill-chain: movimento lateral, coleta, exfiltração, e comando e controle, demonstrando a capacidade de resposta e de contenção de danos da ReaQta também nos últimos estágios de um ciberataque.

A taxa de capacidade de tomada de ação destacou a capacidade da plataforma em reduzir o ruído ao diminuir o número de alertas gerados. A plataforma capturou todas as táticas e técnicas em poucos alertas correlacionados, em vez de gerar um alerta por tática e técnica, o que resultaria em um número inimaginável de alertas para a equipe SOC analisar e responder.

Tomada de ação em alertas

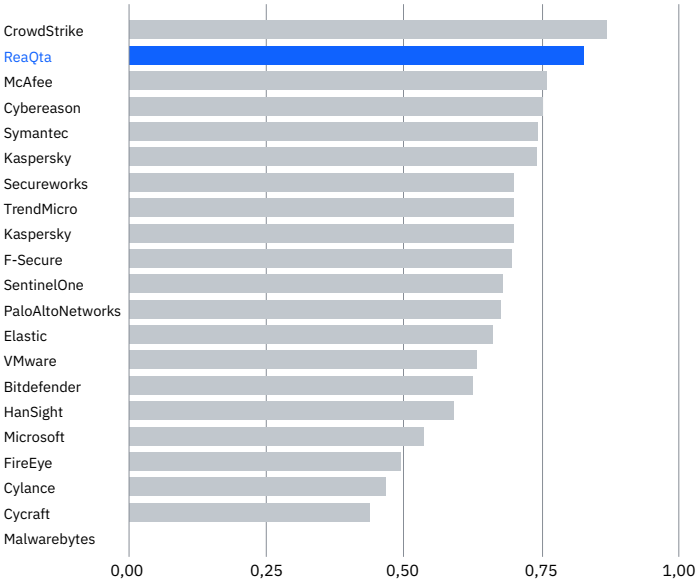


Capacidade acionável dos alertas (dados incluem detecções manuais para fornecedores utilizando MSSPs)

Mais uma vez a ReaQta fornece alertas de alta qualidade, sem intervenção humana, enquanto o primeiro e terceiro fornecedores dependeram de análise manual durante a avaliação.

A quantidade de visibilidade fornecida pela ReaQta torna necessário filtrar dados, correlacioná-los e gerar a menor quantidade de alertas possível, cada um contendo a maior quantia de informações relacionadas. Este é o objetivo dos mecanismos de IA da ReaQta: coletar, correlacionar e resumir a telemetria. A qualidade dos alertas também foi confirmada pela análise da Forrester no gráfico abaixo.

Qualidade dos alertas



Qualidade dos alertas (dados incluem detecções manuais para fornecedores utilizando MSSPs)

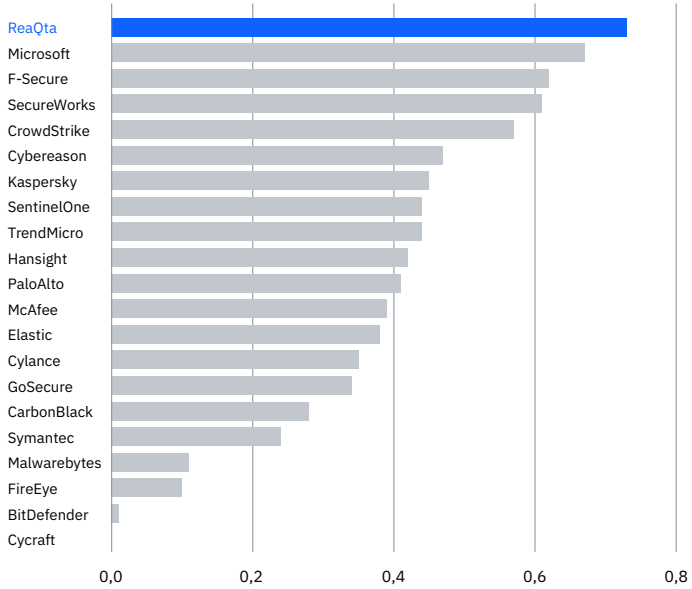
“A capacidade acionável é o produto da eficiência e qualidade dos alertas [...] a eficiência dos alertas (baixa quantidade) e a qualidade dos alertas (o quanto eles ajudarão a entender a narrativa) estão relacionados e são essenciais para compreender o quão ‘acionável’ será um determinado alerta.”

Forrester[2]

Fornecer alertas abrangentes e de alta fidelidade é o critério que distingue uma boa plataforma de meras geradoras de ruído.

O gráfico abaixo mostra como a ReaQta se comportou em comparação com outras soluções quando as detecções manuais foram removidas. Cada barra representa a quantidade de informação relacionada a incidentes capturada a cada alerta gerado. Os mecanismos da ReaQta capturaram a maior quantidade de informação, que resulta em uma redução considerável da carga de trabalho em ambientes reais.

Cobertura do ataque por alerta gerado (relação sinal-ruído)



Porcentagem de cobertura de ataque fornecida por alerta

A ReaQta gerou 25 alertas e coletou todas as informações necessárias corretamente para rastrear os invasores em cada um deles, em vez de criar 158 alertas, um para cada técnica testada.

A capacidade de fornecer um fluxo de trabalho unificado para resolução de incidentes é essencial para reduzir a fadiga de alertas.

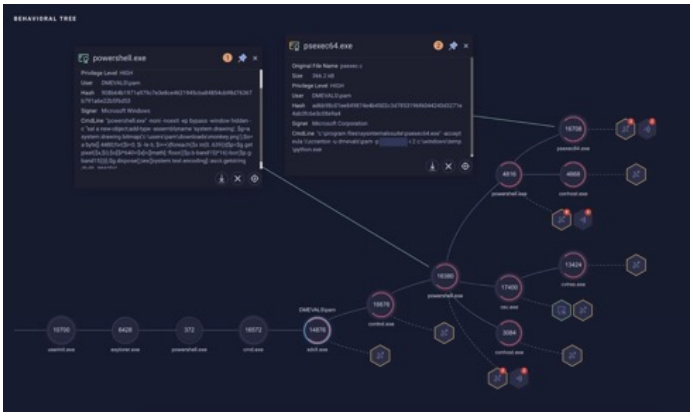
A ReaQta correlacionou a narrativa durante a avaliação MITRE. Isso permitiu que os analistas facilmente entendessem e estudassem um invasor ativo, sem a distração de centenas de alertas sendo gerados, sem correlação direta com o incidente original. Isso teria sido muito mais difícil de processar durante uma análise real.

A abordagem da ReaQta reduziu a fadiga de alerta em 85% e preservou a visibilidade completa durante todo o ataque. A ReaQta foi desenvolvida especificamente para gerar a quantidade mínima de alertas por incidente, proporcionando uma experiência de análise ininterrupta e sem dificuldades. A capacidade de manter todas as informações em uma única visualização ajuda os analistas a responder mais rápido, sem precisar trocar de telas para ter compreensão total dos eventos.

Tenha visibilidade completa de seus terminais para permitir respostas rápidas em todas as etapas

A plataforma foi capaz de manter a correlação entre ações em todos os estágios da kill chain ATT&CK. A correlação automática de eventos reduz o tempo necessário para descobrir diferentes ações executadas pelos invasores e reduz o tempo de resposta no caso de ataques reais.

Árvore comportamental



Linha narrativa correlacionada com ReaQta durante a avaliação MITRE

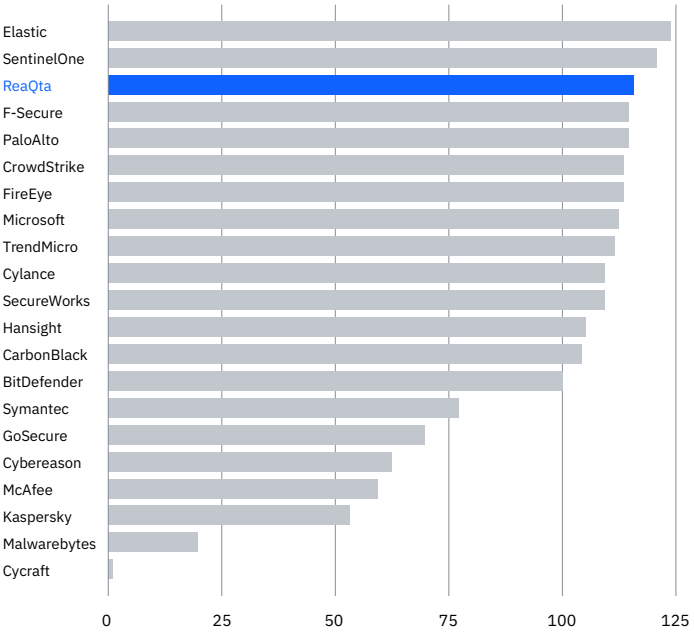
Para fornecer um exemplo relacionado à avaliação, o gráfico acima mostra como fase inteira do ataque foi capturada em um único alerta. A ReaQta correlacionou toda a informação em uma linha narrativa compreensível, proporcionando à equipe SOC todas as informações para uma triagem adequada. Nenhuma interação humana foi necessária e o ataque foi claramente explicado e seu risco avaliado, sem necessidade de qualquer atividade manual.

Observando mais de perto a detecção das táticas e técnicas do APT29, a ReaQta forneceu visibilidade logos nas primeiras etapas da kill chain até os estágios mais sofisticados, geralmente mais difíceis de se detectar. É importante observar que a capacidade da plataforma em detectar ameaças de maneria uniforme em todas as etapas, assim proporcionando oportunidades de resposta e correção em todas as etapas.

A ReaQta mostrou uma das melhores telemetrias em conjunto com um impressionante mecanismo IA capaz de condensar informação e avaliar riscos. Ele se mostrará uma ferramenta poderosa nas mãos de qualquer SOC ou equipe que queira investir seu tempo caçando ameaças em vez de gerenciar alertas constantemente.

A ReaQta demonstrou uma das melhores telemetrias.

Telemetria



Valor de telemetria fornecido pela ReaQta

Conclusão

A ReaQta, uma plataforma baseada em IA, fornece às equipes de segurança recursos para detecção avançada e resposta rápida, minimizando a intervenção humana, simplificando todo o processo de segurança cibernética e promovendo a continuidade de negócios para organizações de todos os tamanhos.

Esta avaliação validou a abordagem da ReaQta para detecção de agentes de ameaça avançados. ReaQta continuará participando de testes independentes no futuro.

A ReaQta reconhece e valoriza o trabalho da MITRE em ajudar organizações a tomar decisões bem informadas graças a essas avaliações.

Para mais informações, acesse:
ibm.com/products/reaqta

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

Produzido nos Estados Unidos da América
Março de 2022

1 Avaliação MITRE ATT&CK, The MITRE Corporation e MITRE Engenuity, 2020.
2 Further Down the Rabbit Hole With MITRE’s ATT&CK Eval Data, Forrester blog, 4 de maio de 2020.