Quantidade não é igual a qualidade.

Symantec Enterprise – um poderoso aliado para nossos clientes

Por: Kevin Haley. Director, Symantec Security Response

A avaliação MITER ATT & CK® fornece dados poderosos para aqueles que podem colocar os resultados no contexto de suas redes e as necessidades de seus SOCs. O MITER não declara um vencedor e, em vez disso, simplesmente incentiva a participação. Infelizmente, muitos fornecedores pegaram um único resultado bruto com algum atributo de topo de gráfico e o declararam um ponto de prova. Esse ponto de prova é então usado para transformar um relatório que é uma avaliação em um concurso e se declarar vencedores. Sem o contexto do mundo real, esta é uma vitória vazia, ou como alguns podem chamá-la: Marketing!

Os resultados da avaliação MITER ATT & CK® nos dão, como fornecedores, uma ideia sólida de como podemos melhorar. Oferece aos clientes uma visão da capacidade de seu produto de defendê-los contra essas ameaças. E pode ajudar um cliente a comparar produtos, mas não sem julgar os resultados dentro do contexto de usabilidade, complexidade e customização necessária. Declarar um produto melhor baseado apenas na quantidade de alertas, por exemplo, significa que a qualidade não é considerada. E provavelmente o “vencedor” é um produto barulhento e inutilizável.

“Os resultados da avaliação MITER ATT & CK® nos dão, como fornecedores, uma ideia sólida de como podemos melhorar”

Por exemplo, nem todas as detecções são iguais. Especialmente detecções que dependem do SOC para criá-las. A avaliação MITER ATT & CK® permite adicionar detecção personalizada. Nenhum desacordo aqui. Mas alguns fornecedores têm expectativas muito altas sobre a capacidade de seus clientes de escrever scripts personalizados. O que não é medido é o esforço para escrever esses scripts. Qualquer pessoa no SOC pode criar esse script ou ele requer um diploma avançado ou um treinamento extensivo? Os fornecedores que chegam ao topo dos resultados dependendo do SOC para escrever scripts complicados realmente apenas transferiram o fardo da detecção para os clientes que afirmam proteger ... quem está fornecendo o valor aqui?

Então, você pode usar a avaliação para saber qual produto é o melhor? Este é provavelmente o objetivo errado. Mas você pode ter uma excelente ideia de quão bom é um produto em um cenário de ataque realista. Vejamos os alertas. Superficialmente, parece que quanto mais alertas você produz sobre ataques em potencial, melhor. Mas qualquer pessoa que trabalhe em um SOC sabe que mais não é melhor quando se trata de alertas. Especialmente quando o fornecedor alerta sobre todas as instâncias de um arquivo sendo compactado ou cada comando do PowerShell sendo executado. Apenas olhar para todos esses alertas sobrecarregaria um SOC. Ninguém tem recursos para examinar tantos alertas.

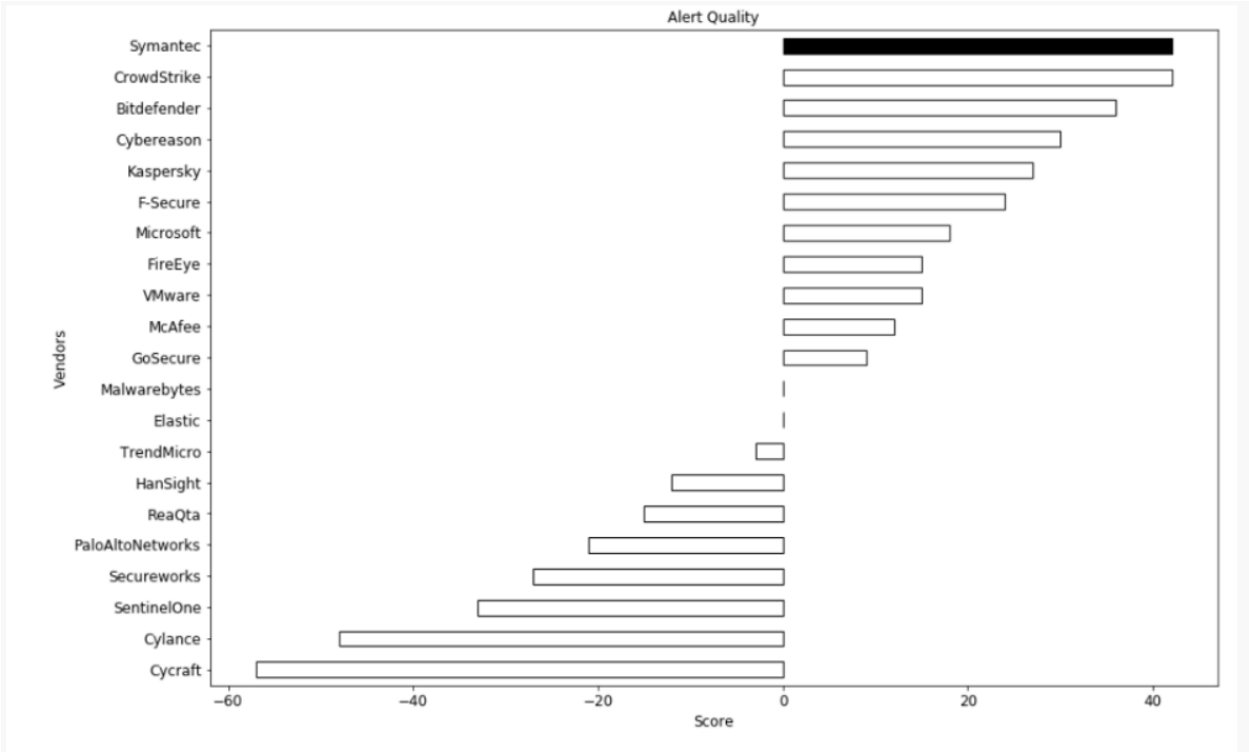
“Mas qualquer pessoa que trabalhe em um SOC sabe que mais não é melhor quando se trata de alertas.”

É claro que ter o menor número de alertas provavelmente também não é uma coisa boa. Uma maneira de ver esses resultados é que a maioria dos fornecedores é muito quente ou muito frio. A sopa fica melhor quando a temperatura está boa.

Tentamos criar um modelo para ajudar a entender os resultados. Não é quem tem mais ou menos alertas. São os fornecedores que fazem a coisa certa. Queremos medir a qualidade dos alertas, não a quantidade.

Analisamos e atribuímos um valor aos tipos de alerta. Atribuímos um alto valor às técnicas críticas alertadas. Coisas como: Credential Dumping, UAC Bypass, Exfiltration, Service Execution e Persistence. Usamos uma pontuação de 3+. Você pode querer usar uma pontuação mais alta ou mais baixa.

Para alertas que não indicam uma técnica crítica sendo usada para promover um ataque como: File and Directory Descovery, Commonly Used Ports, Query Registry and File Deletion, atribuímos -3. Novamente, você deve definir a pontuação de acordo com o que achar correto. Mas de acordo com os nossos anos de experiência em caça de ameaças, isso parecia certo para nós.



Agora temos uma medição da eficácia de nossos produtos. E sabemos que estamos no caminho certo com nossa estratégia de produtos. Estamos construindo detecções de alta qualidade que são acionáveis, que ajudam a focar o SOC em eventos que são importantes e fornecendo a eles as ferramentas para analisar e responder. Esse é o nosso objetivo, ser aliados poderosos do SOC, não dando a eles mais trabalho. Nosso foco não é vencer esses exercícios de “marketing”, mas sim fazer com que nossos clientes sejam os vencedores.

“Se você quiser tentar fazer isso sozinho, ajuste os números ou use este modelo para outras partes da avaliação dos resultados, o script pode ser baixado aqui”

Sobre o Autor:

Kevin Haley. Director, Symantec Security Response

Kevin Haley é responsável por garantir que o conteúdo de segurança da Global Intelligence Network da Symantec seja acionável para seus clientes, incluindo o foco na educação em questões de segurança e incorporando o conteúdo de segurança aos produtos corporativos da Symantec.

.