AVALIAÇÕES MITRE ATT&CK - APT29

Resultados da Trend Micro

SOBRE O MITRE ATT&CK

A MITRE ATT&CK é uma base de conhecimento público de táticas e técnicas adversárias, que pode ser usada como fundação para o desenvolvimento de modelos e metodologias específicos de ameaças cibernéticas. Resumindo, auxilia o mercado a definir e padronizar como descrever a abordagem de um invasor. A MITRE ATT&CK coleta e categoriza táticas, técnicas e procedimentos (TTPs) de ataque comuns e, em seguida, organiza essas informações em um framework. Este framework pode ser usado para ajudar a explicar como os adversários se comportam, o que estão tentando fazer e como.

Ter uma linguagem e estrutura comuns é importante para a habilidade de se comunicar, compreender e responder às ameaças da maneira mais eficiente e eficaz possível. Também ajuda as equipes de SOC/RI a entender que cobertura têm contra várias técnicas de ataque. O framework é atualizado regularmente com novas técnicas fornecidas por profissionais do setor de cibersegurança, incluindo a Trend Micro. As avaliações do MITRE ATT&CK focaram os sistemas Enterprise Matrix para Windows, no entanto, existem várias matrizes de framework:

- Enterprise (Microsoft® Windows®, macOS®, Linux®)
- Cloud (Microsoft® 365®, AWS, Microsoft® Azure™, Google Cloud Platform™, Software as a Service (SaaS))
- Mobile (Android™, iOS)
- Sistemas de Controle Industrial (ICS)

Data

Resultados da avaliação publicados em 21 de abril de 2020.

Evento

Avaliação de terceiros sobre a capacidade de um fornecedor de detectar comportamentos adversos.

https://attackevals.mitre.org/evaluations_html?round=APT29

Soluções Trend Micro inclusas nesta avaliação

- Trend Micro Apex One™ as a Service with Endpoint Sensor (produto primário)
- Trend Micro™ Deep Security™ enterprise
- Trend Micro™ Deep Discovery™ Inspector
- Trend Micro™ Managed XDR Service

RESULTADOS DA AVALIAÇÃO DA TREND MICRO COM O MITRE ATT&CK

Como funciona a avaliação:

MITRE ATT&CK oferece um ambiente de testes para os fabricantes instalarem seus produtos. Dado que a avaliação verifica o comportamento pós-comprometimento, os fornecedores devem configurar seus produtos no modo de detecção ou "somente alerta". Em seguida, uma simulação de um ataque de ameaça persistente avançada (APT) é executada e a solução do fornecedor é avaliada por quais tipos de técnicas ela é capaz de detectar com base na MITRE ATT&CK Matrix for Enterprise. Cada avaliação analisa um cenário de ataque diferente no estilo de um grupo adversário do mundo real.

Esta avaliação emulou um comportamento semelhante ao APT29. O APT29 (também conhecido como Cozy Bear e The Dukes) é um grupo de ameaças que foi atribuído ao governo russo, operando pelo menos desde 2008. Esse grupo supostamente comprometeu o Comitê Nacional Democrata nos EUA, ao longo dos meses de junho a agosto de 2015. O APT29 se distingue pelas implementações furtivas e sofisticadas de técnicas por meio de um arsenal de malwares personalizados.

Resultados gerais para a Trend Micro

- **A Trend Micro foi colocada em primeiro lugar nas detecções,** com base nas configurações iniciais do produto – taxa de detecção de 91%.
    - A avaliação permitiu que os fornecedores fizessem ajustes no produto após uma primeira execução do teste para aumentar suas taxas de detecção em um novo teste. Os resultados do MITRE ATT&CK refletem as taxas de detecção do fornecedor após todos os ajustes do produto, onde tivemos a segunda maior cobertura de taxa de detecção geral.
- **O menor número de detecções perdidas** entre todos os fornecedores (para configuração inicial).
- **Detecções de técnicas fortes,** que é um tipo de detecção de maior credibilidade.
- **Volume de alertas gerenciados.** Um nível mais baixo de alertas combinado com uma alta taxa de detecção significa que podemos reduzir o ruído e evitar a fadiga de alertas para equipes sobrecarregadas.
- **Grande quantidade de telemetria coletada** – telemetria = visibilidade. A Trend Micro coletou 103 peças de telemetria e, nessa medida, estava entre os principais fornecedores.
- **Melhoria na taxa de detecções com o Managed Detection and Response (MDR);** no entanto, os resultados de cobertura de detecção teriam sido muito bons mesmo sem nosso serviço MDR.

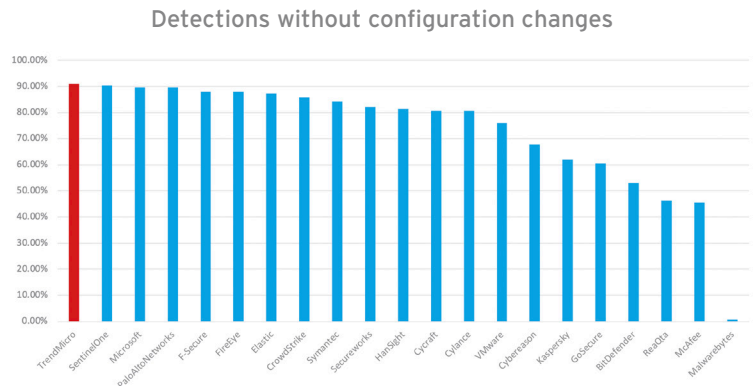
Considerações adicionais

- Detecção e resposta automatizadas.
    - Esta avaliação testa apenas a detecção após um evento. Em pelo menos 10 etapas desse ataque direcionado, a detecção e resposta automatizadas da Trend Micro teriam interferido e interrompido o ataque com uma ação de bloqueio (processo de eliminação, quarentena, isolamento etc.)
- A plataforma Trend Micro™ XDR não fez parte desta avaliação
    - Correlação e contexto são as principais áreas de foco para XDR

Resultados completos aqui: https://attackevals.mitre.org/APT29/results/trendmicro/

FAQS

Você pode explicar as taxas de detecção?



Essa avaliação permitiu que os fornecedores fizessem ajustes no produto após uma primeira execução do teste para aumentar suas taxas de detecção em um novo teste. Os resultados finais mostrados refletem suas taxas de detecção após todos os ajustes do produto. Quando você considera a detecção conforme fornecido originalmente, tivemos a melhor cobertura entre os 21 fornecedores. Acreditamos que esta é uma boa maneira de considerar os resultados por alguns motivos:

- Depois que o teste inicial é feito, os fornecedores avaliam os resultados e, em seguida, podem fazer alterações de configuração de front-end (UX) e back-end (detecção) e o teste é executado novamente. Os ajustes do produto podem variar em importância e podem, ou não, estar imediatamente disponíveis no produto atual dos fornecedores.
- É mais fácil se defender uma vez que você sabe o que o invasor fará. No mundo real, os clientes não têm uma segunda chance contra um ataque.

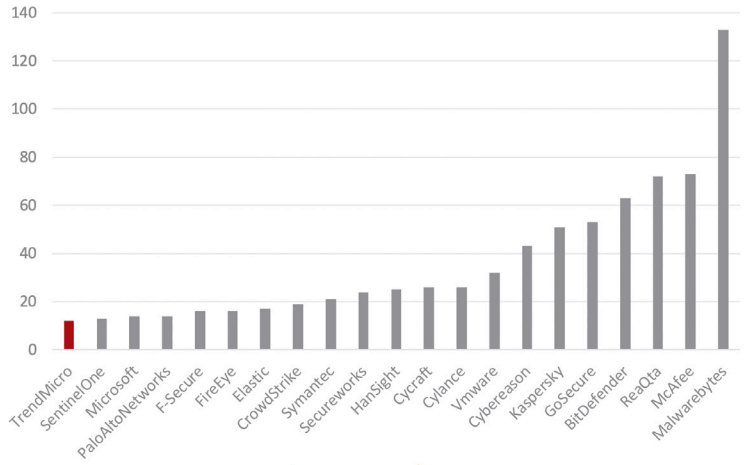
Sem fazer qualquer tipo de exclusão aos dados, e apenas pegando os resultados do MITRE ATT&CK em sua totalidade, tivemos a segunda maior taxa de cobertura de detecção. Considerando nossas detecções coletivas, em comparação com o número total de etapas avaliadas, tivemos mais de 91,79% de cobertura de detecção e ficamos em segundo lugar no pool de 21 fornecedores – mostrando um grande equilíbrio de recursos de detecção em toda a cadeia de ataques.

O que aconteceu com as 11 detecções que perdemos (listadas como "Nenhuma")?

As falhas de detecção estão do outro lado da equação de cobertura de detecção. Como tivemos uma ótima cobertura, tivemos poucas falhas. Fomos extremamente bem contra a concorrência, em termos de número de detecções perdidas. Apresentamos o menor número dessas detecções (12) entre todos os fornecedores, com base na configuração inicial do produto, além de termos o segundo menor (11) nos resultados finais, após ajustes do produto.

Lembre-se de que essas detecções não são ataques individuais, são pequenos passos em um ataque maior. Não é necessário detectar todas as etapas do ataque para detectá-lo e responder adequadamente. Independentemente disso, esse teste nos permite identificar áreas para melhorar o produto e, como resultado, alguns itens relacionados a detecções perdidas estão agora na fila de desenvolvimento.

Fewest Missed Detections — Initial Configuration



O que significa mudança na configuração?

Nesses casos, algo pode não ter sido identificado, mas o produto foi capaz de detectá-lo com uma alteração na configuração. O fornecedor fez um ajuste no produto e a detecção aconteceu em uma segunda tentativa.

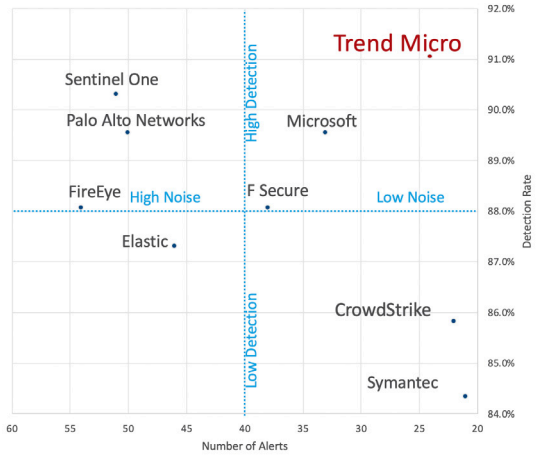
Conforme observado acima, as alterações de configuração não tiveram um impacto material em nossos resultados gerais de cobertura de detecção. Na verdade, quando você compara fornecedores, removendo os resultados de detecção das alterações pós-configuração, a Trend Micro é colocada em primeiro lugar para a identificação geral inicial. Esta é outra área em que as alterações de configuração feitas durante o teste nos ajudaram a identificar e iniciar melhorias no produto.

O número de alertas da Trend Micro é menor: por que isso é bom?

À primeira vista, alguns podem esperar que tenhamos o mesmo número de alertas que detecções. No entanto, nem todas as detecções representam problemas iguais e nem tudo deve ter um alerta. Em grande quantidade, podem levar à fadiga de alertas e aumentar a dificuldade de classificar o ruído para chegar ao que é mais importante. Por exemplo, um dos fornecedores na avaliação disparou 90 alertas individuais do ataque APT, criando um número excessivo de itens para um analista de segurança fazer a devida triagem.

Em comparação, a Trend Micro tinha um terço desses alertas, tornando mais gerenciável para a segurança revisar e chegar ao que era importante. Quando você os considera associados às nossas detecções de alta fidelidade, a Trend Micro teve excelente desempenho na redução do ruído de todas as detecções em um número mínimo de alertas significativos.

Highest Initial Detection, Low Alert Volume
(Selected vendors shown)



Qual é a diferença entre "Geral", "Tática" e "Técnicas"? A Trend Micro parecia estar com pouco Geral e não tinha detecções de Tática; isso é um problema?

https://attackevals.mitre.org/APT29/detection-categories.html

Existe uma hierarquia natural no valor dos diferentes tipos de detecções:

- Uma detecção Geral indica que algo foi considerado suspeito, mas não foi atribuído a uma tática ou técnica específica.
- Uma detecção na Tática significa que a detecção pode ser atribuída a um objetivo tático (por exemplo, acesso à credenciais).
- Uma detecção na Técnica significa que a detecção pode ser atribuída a uma ação adversária específica (por exemplo, dumping de credenciais).

Temos detecção forte em Técnicas, que é uma medida de detecção melhor. Com a Técnica individual MITRE ATT&CK identificada, a Tática associada pode ser determinada, pois normalmente há apenas algumas Táticas que se aplicariam a uma Técnica específica. Ao comparar os resultados, você pode ver que muitos fornecedores tiveram detecções de Tática mais baixas no todo, demonstrando um reconhecimento geral de onde deveria estar a prioridade. O fato de termos detecções Gerais mais baixas em comparação com detecções de Técnica é positivo.

Na execução inicial do teste, coletamos 103 peças de telemetria, o que nos coloca entre os fornecedores de primeira linha (o intervalo de telemetria coletado entre os fornecedores foi de 1 a 113). Isso demonstra que oferecemos aos analistas de segurança acesso ao tipo e profundidade de visibilidade de que precisam ao examinar detalhadamente a atividade do invasor.

Quanto o MDR influenciou os resultados?

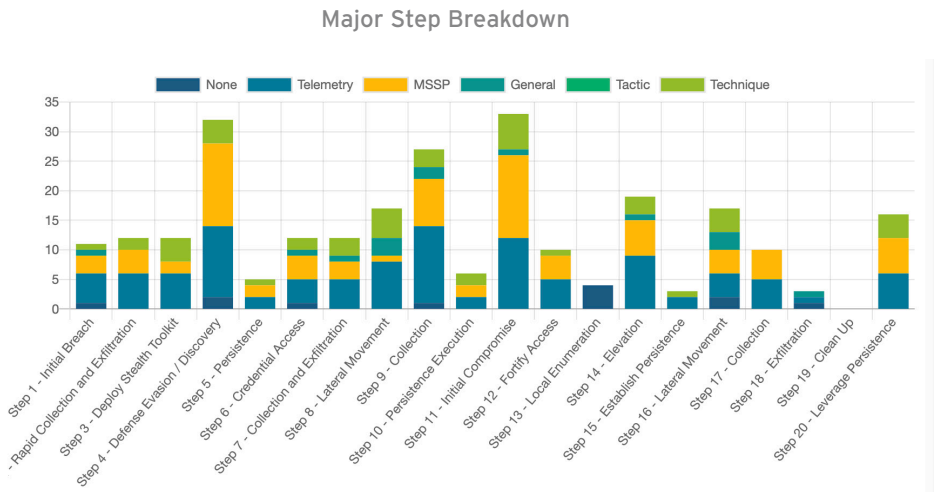
Os analistas do Trend Micro MDR contribuíram para a "detecção atrasada" ou categoria MSSP. É aqui que a detecção envolveu ação humana e pode não ter sido iniciada automaticamente. Nossos resultados mostram a força de nossos analistas de MDR. Se um serviço MDR foi incluído nesta avaliação, o ideal é que ele fornecesse uma boa cobertura, pois demonstra que a equipe é capaz de detectar eventos com base na telemetria coletada.

É importante observar que os números da detecção atrasada não significam necessariamente que foi a única maneira pela qual uma detecção foi ou poderia ser feita: a mesma detecção pode ser identificada por outros meios. Nossos resultados mostram a força de nossos analistas de MDR, no entanto, nossos resultados de cobertura de detecção teriam permanecido fortes sem esse envolvimento humano – aproximadamente 86% de cobertura de detecção.

As detecções correlacionadas da Trend Micro parecem baixas, por quê?

A categoria de prioridade para esta avaliação são as detecções principais. A correlação se enquadra na categoria "detecção de modificador", que analisa o que acontece além de uma detecção inicial.

Dado que nossa plataforma XDR não fez parte desta avaliação, assim como a correlação entre as camadas de segurança – segurança de e-mail, por exemplo, não estava no escopo – há um valor de correlação que podemos fornecer aos clientes além do que está representado aqui.



Onde podemos contar com o Deep Discovery Inspector?

A maioria das atividades relacionadas a esta simulação APT29 aconteceu dentro do próprio host, portanto, havia apenas um punhado de coisas relacionadas à rede.

Ao contrário dos produtos de muitos concorrentes, o Apex One já vê eventos de rede de seus recursos de sistema de proteção de vulnerabilidade host-based intrusion prevention system (HIPS) e kernel hooks de reputação na web. O Deep Discovery Inspector e o Apex One detectaram um número de atividades de rede e, em última análise, o Deep Discovery Inspector forneceu duas detecções exclusivas. Nossos resultados teriam permanecido muito fortes sem ele – cobertura de detecção de aproximadamente 90,2%.

Por que o Deep Security foi incluído?

O cenário de ataque incluiu alguns servidores Windows, portanto, o Deep Security estava no escopo desta avaliação. Além disso, como o Deep Security está em um servidor Active Directory, teve alguma visibilidade da atividade do endpoint por meio da inspeção de log nos logs do Active Directory.

O que deve ser considerado ao observar os resultados da Trend Micro? O que o teste não considera?

É importante reconhecer que essa avaliação testa apenas a detecção após um evento. Como resultado, ela não mede ou leva em consideração nenhuma detecção automatizada e medidas de resposta. Isso é significativo para a Trend Micro, pois nossa filosofia é bloquear e prevenir o máximo possível, para que os clientes tenham menos questões para solucionar e resolver. Nosso produto não foi originalmente projetado para esse tipo de parâmetro de teste, então, em alguns casos, não gravamos uma atividade (temos uma opção apenas de detecção) porque a teríamos bloqueado. Este teste não mostra isso.

Em pelo menos 10 etapas do ataque direcionado, a detecção e a resposta automatizadas teriam intervindo, interrompendo o ataque com uma ação de bloqueio (processo de eliminação, quarentena, isolamento e etc.).

Da mesma forma, no caso de muitos APTs, provavelmente teria começado com um esforço de engenharia social (por exemplo, e-mail de phishing), que provavelmente teria sido detectado anteriormente por nossa segurança de e-mail. O MITRE ATT&CK não testa no ponto de acesso inicial, portanto, a segurança neste estágio da cadeia de eliminação não é avaliada.

Também é importante observar que essa avaliação analisou apenas endpoints e servidores no Windows; ela não olhou para o Linux, onde, é claro, a Trend Micro tem vantagens sobre outros fornecedores.

Como oTrend Micro XDR se aplica a esta avaliação MITRE ATT&CK?

A plataforma XDR, que foi disponibilizada no final de junho de 2020, não fez parte da avaliação. Existem várias vantagens do XDR:

- Detecções correlacionadas com base em regras que procuram comportamentos diferentes nas camadas de segurança
- Menos alertas acionáveis com maior contexto MITRE ATT&CK
- Visibilidade e investigação integrada em todas as camadas de segurança – endpoint, e-mail, rede, servidores e workloads em nuvem.

Nenhuma outra consideração do produto está incluída na avaliação, por exemplo, não avalia o desempenho, falsos positivos, custo de propriedade, integração com outras ferramentas, interface do usuário, políticas de segurança, visão do produto, roteiro e outros fatores que podem ser importantes critérios de seleção para organizações.

Existe um vencedor ou líder para os resultados? Por que outros fornecedores estão dizendo que obtiveram as melhores pontuações, as avaliações mais altas etc.?

O MITRE ATT&CK não pontua, classifica ou fornece comparação lado a lado de produtos. Os fornecedores devem pegar os resultados brutos e analisar os dados para calcular as pontuações e entender seus resultados em comparação com outros fornecedores. Existem muitas maneiras de avaliar os dados, algumas mais realistas e diretas do que outras.

Obtivemos resultados gerais realmente bons e pontuamos fortemente em muitos dos parâmetros testados e de acordo com várias das maneiras como os dados podem ser visualizados. Com mais de 91% de cobertura de detecção, mostramos um grande equilíbrio de recursos de detecção. Nossos resultados também apoiam nossa estratégia de fornecer detecções de maior fidelidade, enquanto gerenciamos volumes de alerta.

OUTRAS INICIATIVAS MITRE ATT&CK COM A TREND MICRO

O que mais fazemos com o MITRE ATT&CK?

A Trend Micro trabalha em estreita colaboração com a organização MITRE ATT&CK e contribui regularmente com o framework MITRE ATT&CK compartilhando quaisquer novas técnicas não listadas atualmente em suas matrizes. Tanto a Trend Micro quanto a Trend Micro™ Zero Day Initiative™ (ZDI) são Numbering Authorities (CNA) do Common Vulnerability Exposures (CVEs®). A Trend Micro pode emitir CVEs para vulnerabilidades especificamente para produtos da Trend Micro (eles não precisam ser encontrados por nós). O ZDI pode emitir CVEs para produtos que ainda não são cobertos por outro CNA. Fazemos parte de vários grupos de trabalho com o MITRE ATT&CK e outros colegas do setor que trabalham com questões relacionadas a vulnerabilidades.

Quais recursos de produto a Trend Micro possui em relação ao MITRE ATT&CK?

- O Apex One mapeia os logs de detecção para táticas, técnicas e procedimentos MITRE ATT&CK. Existem vários mapeamentos que podem ser vistos no painel de detecção ou no registro de detecção.
- A Trend Micro Cloud One™ e o Deep Security referenciam IDs MITRE ATT&CK diretamente no sistema de prevenção de intrusões(IPS), monitoramento de integridade e regras de inspeção de logs. No futuro, planejamos publicar um mapa da nossa cobertura.
- O Trend Micro™ Tipping Point™ faz referência a IDs MITRE ATT&CK em regras e fornece mapeamento estendido no arquivo de referências .xml (comumente conhecido como dvreferences.xml).
- O Deep Discovery também mapeia os resultados da detecção para táticas e técnicas da MITRE ATT&CK Matrix a fim de fornecer maior percepção e visibilidade dos métodos e vetores usados ao longo do ciclo de vida do ataque.
- O Trend Micro™ Cloud App Security mapeia detecções para técnicas na nuvem (Microsoft 365®) MITRE ATT&CK Matrix.
- O Trend Micro™ XDR inclui:
    - Visualizações específicas do framework MITRE ATT&CK para mapear com tela inteira da ferramenta em detecção e telemetria aprimoradas.
    - Hunting com técnicas individuais, critérios personalizados descritos sequencialmente (coleção de técnicas de ataque específicas) e suporte a arquivos SIGMA.

Agora que você entende os resultados e a estrutura, é importante saber como você pode aproveitar as informações.

Muitas organizações estão começando a usar o MITRE ATT&CK para melhorar suas operações de segurança, certificando-se de que estão adequadamente equipadas para o comportamento adversário comum. Você pode usá-la para avaliar seus processos e recursos para identificar quaisquer lacunas, mas também sobreposições na cobertura que podem estar causando custos operacionais extras. Se você encontrar essas falhas poderá olhar para avaliações como esta, para ver quais soluções podem ajudar a solucioná-las. À medida que o cenário de ameaças continua mudando e evoluindo, o MITRE ATT&CK fornece uma linguagem e contexto comuns para que as empresas perguntem aos fornecedores sobre seus recursos, tornando mais fácil eliminar o ruído e obter a melhor segurança.

TREND MICRO™

Securing Your Connected World