AUTOFOCUS

Transforme sua inteligência contra ameaças em arma letal.

O serviço de inteligência de ameaças AutoFocus da Palo Alto Networks acelera a análise de ameaças e o fluxo de trabalho de caça aos ataques mais prejudiciais, exclusivos e direcionados. A segurança hospedada amplia a plataforma de segurança da Palo Alto Networks com a visibilidade e o contexto de ameaças necessários para responder a ataques críticos de maneira mais rápida, sem acrescentar recursos de segurança de TI adicionais.

Transforme a sua inteligência contra ameaças em arma letal

- Acelere a análise, a busca e os fluxos de trabalho de resposta a ameaças, incluindo alertas de prioridade para os eventos mais críticos
- Forneça o contexto sobre ataques, adversários e campanhas, incluindo os setores visados
- Amplie a plataforma de segurança da Palo Alto Networks, com contexto de ameaça uma parte nativa do PAN-OS e Panorama, incluindo uma API aberta para integração em sistemas de segurança de terceiros

Ampliação da plataforma da Palo Alto Networks

Os invasores cibernéticos se tornaram bem automatizados e fazem ataques cada vez mais sofisticados em volumes maiores e nunca antes vistos. As sobrecarregadas equipes de segurança não conseguem acompanhar cada ameaça, o que deixa pouco tempo para investigar os ataques realmente avançados. A plataforma exclusiva da Palo Alto Networks® oferece um novo caminho a seguir, que começa com uma abordagem voltada para a prevenção e que coloca a automação novamente nas mãos dos defensores da rede.

Como a nossa plataforma evita a maioria das ameaças, as equipes de segurança podem dedicar seu tempo limitado na busca e nas respostas para o baixo número de ataques realmente avançados e direcionados ao usar o AutoFocus™. O serviço amplia a plataforma com a inteligência global de ameaças e o contexto do ataque necessários para acelerar a análise, a avaliação forense e os fluxos do trabalho de busca. Juntos, a plataforma e o AutoFocus distanciam as equipes de segurança das abordagens antigas que dependem da agregação de um número crescente de alertas focados em detecção e mitigação pós-evento para impedir a maioria dos ataques e possibilitar as atividades de busca proativa.

Alertas de prioridade

O AutoFocus permite que você faça a distinção entre as ameaças mais importantes e os ataques diários de commodities, contextualizando eventos em sua rede ou dados públicos com etiquetas. As etiquetas exclusivas do AutoFocus informam quais famílias de malware, campanhas, agentes de ameaças, comportamentos maliciosos e explorações estão sendo usados contra você. Quando uma etiqueta

corresponde a um evento em sua rede, um alerta de prioridade é enviado por e-mail, dentro do painel do AutoFocus, ou por HTTP post, com o contexto completo da etiqueta incluído. Os alertas são altamente personalizáveis, melhorando o fluxo de trabalho de segurança existente com priorização e contexto para as ameaças mais críticas.

Etiquetas

As etiquetas melhoram a sua visibilidade sobre as ameaças mais críticas provenientes das famílias de malware de inteligência contextual, campanhas, agentes de ameaças, comportamentos maliciosos e explorações. Elas podem ser criadas para qualquer host ou um indicador baseado em rede no AutoFocus, alertando você quando uma ameaça específica é observada em sua organização ou em seu setor. Além de alertas de prioridade, todas as etiquetas são pesquisáveis, permitindo que você consulte instantaneamente amostras ou indicadores maliciosos associados.

Quando novas ameaças são identificadas, a Unit 42, a equipe de pesquisa da Palo Alto Networks, sua própria organização e a comunidade global de especialistas do AutoFocus incluem novas etiquetas ao serviço. As etiquetas proporcionam insights de:

- famílias de malware
- campanhas de ataque
- agentes
- comportamentos maliciosos
- explorações

Equipe de inteligência de ameaças Unit 42

A Unit 42 é a equipe de pesquisa e inteligência de ameaças da Palo Alto Networks, formada por pesquisadores bem-sucedidos de segurança cibernética e especialistas do setor. A Unit 42 coleta, pesquisa e analisa as novas ameaças, fornecendo informações sobre os mais recentes grupos adversários e campanhas e as compartilha com os clientes da Palo Alto Networks e da comunidade de segurança em geral. A Unit 42 adiciona inteligência humana especializada ao AutoFocus por meio da criação de etiquetas com base em sua pesquisa e inteligência de código aberto, que fornece contexto e priorização de ameaças identificadas, ampliando, por sua vez, sua equipe de segurança com o seu conhecimento.

O AutoFocus é a principal ferramenta de análise que a Unit 42 usa para identificar novas ameaças, correlacionar dados globais, identificar conexões entre as amostras maliciosas e criar perfis de campanha ou adversários. Veja a pesquisa mais recente da Unit 42 identificada com o AutoFocus.

Ampliação da plataforma com Threat Intelligence

O AutoFocus ajuda toda a equipe de segurança de TI a se tornar caçadora de ameaças avançadas em vez de depender de um pequeno grupo de profissionais de operações de segurança altamente especializados. A inteligência de ameaças do serviço é disponibilizada diretamente na plataforma da Palo Alto Networks, incluindo o PAN-OS® e o Panorama™. O AutoFocus acelera os fluxos de trabalho existentes da equipe de segurança, permitindo uma investigação aprofundada de atividades suspeitas, sem recursos especializados adicionais.

Quando há necessidade de uma análise mais aprofundada, os usuários podem fazer uma varredura entre o AutoFocus e o PAN-OS ou o Panorama, com buscas já preenchidas para ambos os sistemas.

Com o AutoFocus e a plataforma, os usuários podem responder perguntas sobre:

- o nível de direcionamento ou exclusividade de uma ameaça na rede.
- amostras maliciosas relacionadas para uma investigação mais detalhada.
- histórico da resolução de domínio para identificar consultas de DNS suspeito.

Busca

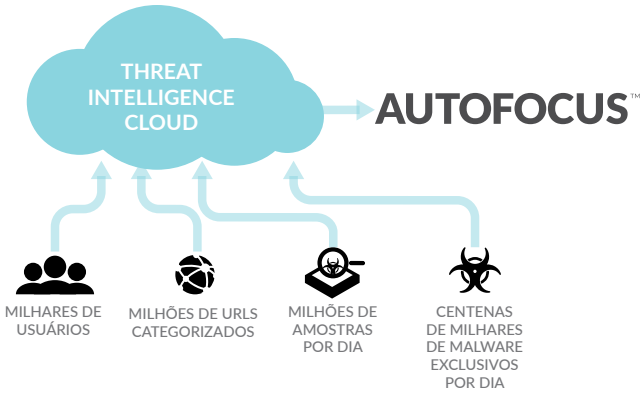
Frequentemente, responder a ameaças direcionadas e exclusivas exige análise humana. Para responder a um comprometimento ativo ou em andamento, é essencial ter uma alta velocidade de investigação e a capacidade de correlacionar dados de maneira significativa. O AutoFocus permite que você construa buscas multicamadas sofisticadas no host e nos níveis de artefatos baseados em rede, e direcione sua busca dentro do setor, do período de tempo e de outros filtros, o que lhe permite fazer conexões anteriormente desconhecidas entre os ataques e dinamizar sua inteligência. O AutoFocus coloca todos os recursos da inteligência de ameaças da Palo Alto Networks em suas mãos, reduzindo radicalmente o tempo que leva para realizar a análise, avaliação forense e busca.

Mecanismo de análise estatística

Ao realizar a análise de ameaças, as equipes de segurança precisam identificar rapidamente quais indicadores de comprometimento (IOCs) representam o melhor caminho para uma investigação adicional. Cada arquivo tem centenas, possivelmente milhares, de artefatos, com apenas um pequeno número de IOCs exclusivos capaz de relacioná-los ao perfil maior de um adversário ou ataques relacionados. O AutoFocus usa um mecanismo de análise estatística inovador, que correlaciona bilhões de artefatos em todo um conjunto de dados globais e apresenta indicadores exclusivos de comprometimento (IOCs) provavelmente associados a ataques direcionados. O serviço aplica automaticamente um sistema exclusivo de ponderação visual para identificar IOCs exclusivos e críticos, direcionando a análise e os esforços de resposta a incidentes para o caminho mais relevante.

Evite ataques exclusivos e direcionados

As equipes de segurança precisam mais do mais que nunca de uma forma de priorizar, analisar e correlacionar inteligência de ameaças; elas precisam de uma forma de transformá-la em controles acionáveis para evitar futuros ataques. O AutoFocus permite que você crie novas proteções para a plataforma de segurança da Palo Alto Networks ao exportar IOCs de alto valor de serviço para listas de bloqueio externo do PAN-OS, bloqueando instantaneamente URLs, domínios ou endereços IP maliciosos. O AutoFocus também pode exportar indicadores para dispositivos de segurança de terceiros por meio de um formato CSV padrão. As equipes de segurança podem usar o AutoFocus para identificar ataques exclusivos e direcionados com os quais sua organização se depara e tomar medidas diretas para mitigá-los e evitá-los.



Arquitetura e fontes de inteligência do AutoFocus

O AutoFocus foi desenvolvido em um ambiente de computação distribuído de larga escala hospedado na nuvem de inteligência de ameaças da Palo Alto Networks. Ao contrário de outras soluções, o serviço torna os dados de ameaças acessíveis e acionáveis ao nível de IOC e vai além de simplesmente mostrar logs resumidos a partir de várias fontes em um painel. O AutoFocus tem uma visibilidade sem precedentes do cenário de ameaças, com o insight coletivo de milhares de empresas globais, provedores de serviços e governos que alimentam o serviço. O serviço se correlaciona e obtém inteligência de:

- WildFire™, o maior serviço de sandbox de rede do setor
- filtragem de URL com o serviço do PAN-DB
- rede DNS passiva global da Palo Alto Networks
- equipe de pesquisa e inteligência de ameaças Unit 42
- feeds de terceiros, inclusive de inteligência de fonte fechada e aberta.

O AutoFocus cria mais de um bilhão de amostras e sessões, incluindo bilhões de artefatos, imediatamente acionáveis para análise de segurança e esforços de resposta.

Integrações simples de terceiros

As equipes de análise de ameaças, avaliações forenses e resposta a incidentes muitas vezes dependem de muitos scripts, ferramentas de código aberto, dispositivos e serviços de segurança para investigar possíveis incidentes. O AutoFocus pode reduzir significativamente o tempo necessário para investigar ao enriquecer os serviços de terceiros com a API do AutoFocus, com a capacidade remota de varredura e o suporte para o formato de dados STIX.

- A API do AutoFocus tem como base uma estrutura RESTful fácil de usar, e permite integrações de centenas de casos de uso, como inserção de inteligência dentro de ferramentas SIEM (Informações de segurança e gestão de eventos) existentes, disponibilizando dados para análise adicional de ameaças ou automações personalizadas de bloqueio de ameaças.
- Os usuários do AutoFocus podem fazer avaliações a partir de indicadores do serviço tanto para sistemas de terceiros internos como de externos diretamente do AutoFocus. As equipes podem definir até 10 sistemas externos, permitindo que eles continuem sua análise ininterruptamente em toda a infraestrutura; assim como correlacionar os logs de firewalls de última geração ou acionar buscas em ferramentas SIEM.
- O AutoFocus oferece integração imediata com infraestrutura de STIX e disponibiliza os dados para exportação no formato de dados STIX.

Manutenção de privacidade

O AutoFocus tem controles rigorosos de privacidade e segurança para impedir o acesso a informações confidenciais ou identificáveis. O serviço só permite que usuários autorizados vejam os dados associados à sua organização, com um mecanismo opcional de "aceitação" para compartilhar dados anônimos com outros usuários. O AutoFocus não permite o acesso a nenhum arquivo proveniente de cliente dentro do serviço, fornecendo somente resultados de análises para amostras observadas na rede de cada respectivo cliente, sem divulgar o conteúdo do arquivo original. Todo o acesso ao serviço ocorre com uma conexão segura e criptografada. O ambiente do AutoFocus baseado em nuvem é monitorado e protegido pela Palo Alto Networks de forma contínua.

Requisitos do AutoFocus

O AutoFocus é oferecido como um serviço hospedado de segurança que não exige mudanças na configuração do seu firewall de última geração da Palo Alto Networks e nem resulta em qualquer impacto adicional no desempenho do dispositivo. Para utilizar o serviço, os clientes devem ter uma conta de suporte válida, e isso vale também para clientes que compraram um firewall de última geração ou a proteção avançada de endpoints Traps™. Como o AutoFocus não depende de hardware e não precisa de quaisquer mudanças no dispositivo, não há necessidade de nenhuma versão específica do PAN-OS ou de qualquer hardware adicional. Recomendamos que seja assinante do WildFire (PAN-OS 4.1 ou superior) para aproveitar completamente o AutoFocus.

Informações de licenciamento

O AutoFocus é oferecido como uma assinatura anual por estação. Fale com seu parceiro ou revendedor da Palo Alto Networks para obter mais informações sobre licenciamento.

4401 Great America Parkway
Santa Clara, CA 95054

Principal: +1.408.753.4000
Vendas: +1.866.320.4788
Suporte: +1.866.898.9087

www.paloaltonetworks.com