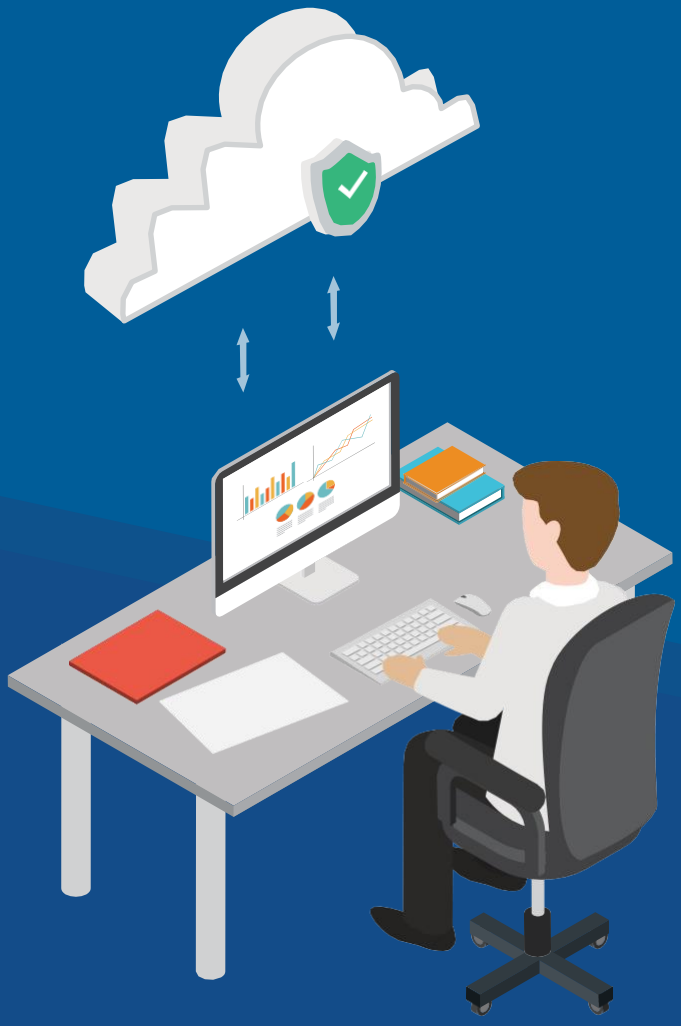
ManageEngine
Log360

Detecção de intrusos de rede com **Processamento de feed STIX/TAXII**

Um Guia



www.manageengine.com/br/log360/

Introdução

No atual cenário tendo ameaças como panorama, a chave para a sua mitigação eficiente é a detecção precoce. A Structured Threat Information Expression (STIX), uma linguagem estruturada para descrever ameaças, e o protocolo Trusted Automated Exchange of Indicator Information (TAXII), uma plataforma colaborativa de compartilhamento de ameaças, surgiram como formas orientadas pela comunidade como uma defesa contra ameaças cibernéticas. Como o STIX e o TAXII fornecem padrões globais para identificar e compartilhar informações sobre ameaças, os feeds de ameaças baseados nesses protocolos são amplamente usados e sempre fornecem as informações mais recentes e confiáveis sobre esse perigo.

A maneira ideal de proteger a rede da sua organização seria atualizar constantemente o banco de dados de ameaças com esses feeds. No entanto, como qualquer administrador de segurança sabe, fazer essa atualização com frequência requer muito trabalho. O Log360, uma solução de gerenciamento de logs e conformidade de TI, tem um processador de feed STIX/TAXII integrado, o que facilita a detecção de ameaças em tempo real.

O processador de feed STIX/TAXII atualiza o banco de dados global de ameaças em instâncias Log360 locais todos os dias, para garantir que seus feeds de ameaças permaneçam atualizados. O banco de dados global de ameaças também contém mais de 600 milhões de endereços IP inseridos na blacklist, coletados de outras fontes abertas confiáveis e atualizados diariamente. O Log360 envia alertas em tempo real sempre que uma fonte inserida na blacklist tenta interagir com sua rede, ajudando você a detectar ameaças com antecedência.

Detecção de ameaças com o Log360

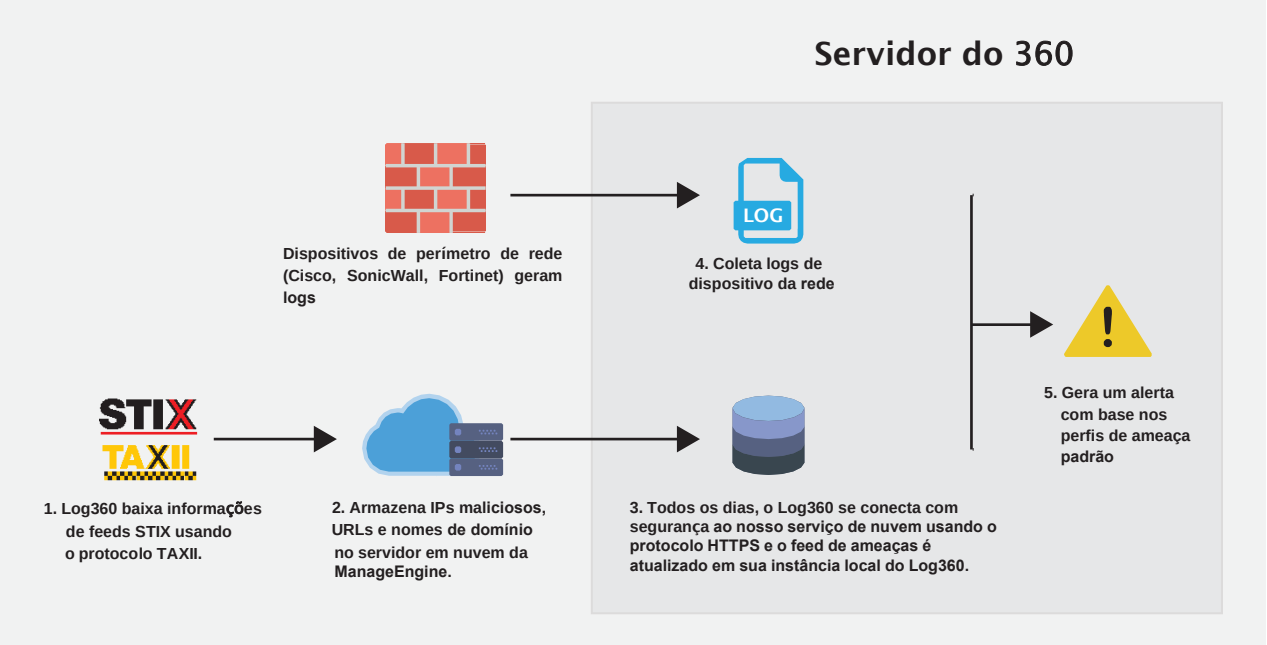
- **Acesse uma base de conhecimento abrangente:** O Log360 processa alguns dos feeds de ameaças mais proeminentes, incluindo aqueles baseados nos protocolos STIX/TAXII.

  Você também pode adicionar os feeds personalizados baseados em STIX/TAXII que sua organização assina.

- **Informações dinâmicas sobre ameaças:** O Log360 extrai automaticamente as informações mais recentes dos feeds de ameaças, garantindo que você se mantenha atualizado.

- **Nenhuma configuração necessária:** O Log360 começa a processar os feeds imediatamente após a implantação.

Como funciona



1 O Log360 baixa os feeds de ameaças diariamente de dois feeds baseados em STIX/TAXII: Hail A TAXII e AlienVault OTX. Se você adicionou outros feeds personalizados, ele também coleta informações sobre ameaças deles.

2 Os feeds de ameaças baixados (compostos por IPs mal-intencionados, URLs e nomes de domínio) ficam armazenados em nosso serviço de nuvem, para que os recursos, a memória e o desempenho do servidor do Log360 não sejam afetados.

3 Todos os dias, às 7 horas, o Log360 se conecta com segurança ao nosso serviço em nuvem usando o protocolo HTTPS e o feed de ameaças é atualizado em sua instância local do Log360.

4 O Log360 coleta os logs de todos os dispositivos em sua rede.

5 Em seguida, ele correlaciona os dados de log com os feeds de ameaças em tempo real, detecta tentativas de invasão de nomes de domínio, URLs ou IPs mal-intencionados, se houver, e envia notificações por e-mail ou SMS para os respectivos profissionais de segurança.

O melhor de tudo é que todo o processo de detecção de ameaças do Log360 listado acima não requer nenhuma configuração de sua parte. Assim que você implanta a solução, seu processador de feed de ameaças começa a funcionar automaticamente.

Em resumo

- **Com quais objetos o processador de feed STIX/TAXII é compatível?** Endereços IP mal-intencionados, URLs e nomes de domínio que são relatados nos feeds STIX são armazenados no banco de dados global de ameaças do Log360.
- Que outras informações o banco de dados global de ameaças possui? Ele também contém mais de 600 milhões de endereços IP inseridos na blacklist coletados de outras fontes abertas confiáveis.
- **Qual protocolo é usado para transferir feeds em nuvem para a instância local?** A instância local do Log360 se conecta ao serviço em nuvem da ManageEngine usando o protocolo HTTPS seguro.
- **Com que frequência os dados de ameaças na instância local são atualizados?** O banco de dados global de ameaças na instância local é atualizado com as informações mais recentes, todas as manhãs às 7 horas.
  Se você adicionou feeds de ameaças personalizados, as informações são recuperadas e armazenadas de acordo com a programação que você especificou.
- **O que é correlacionado para detectar ameaças instantaneamente?** O Log360 correlaciona logs de sua rede com o banco de dados global de ameaças para detectar ameaças.

Adicionando feeds de ameaças personalizados ao Log360

Para adicionar um novo servidor de feed de ameaças:

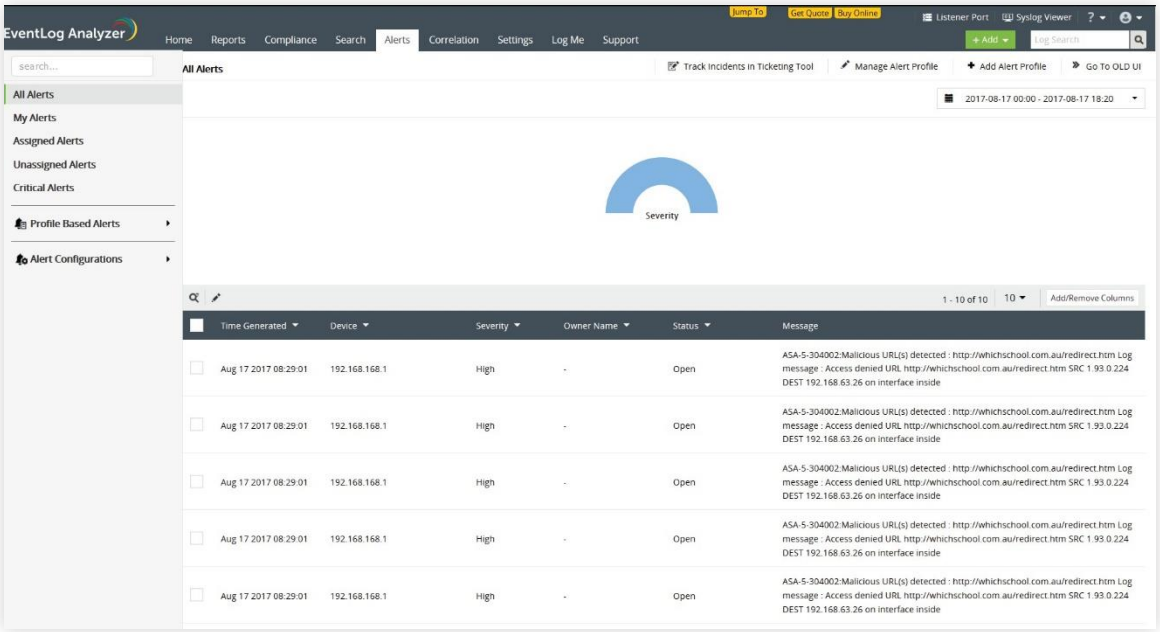
1. Vá para **Configurações** > **Gerenciamento de Ameaças** > **Adicionar Novo Servidor.**
2. Na caixa Adicionar Servidor, digite o nome de exibição, URL, nome de usuário e senha desejados.
3. Na lista suspensa "Cronograma", selecione o tipo de cronograma desejado e o horário exato para a coleta do feed do servidor TAXII.
4. Na caixa "Enquete desde", escolha uma data a partir da qual os feeds anteriores devem ser coletados.
5. Para salvar a configuração do servidor, clique em Adicionar Servidor.

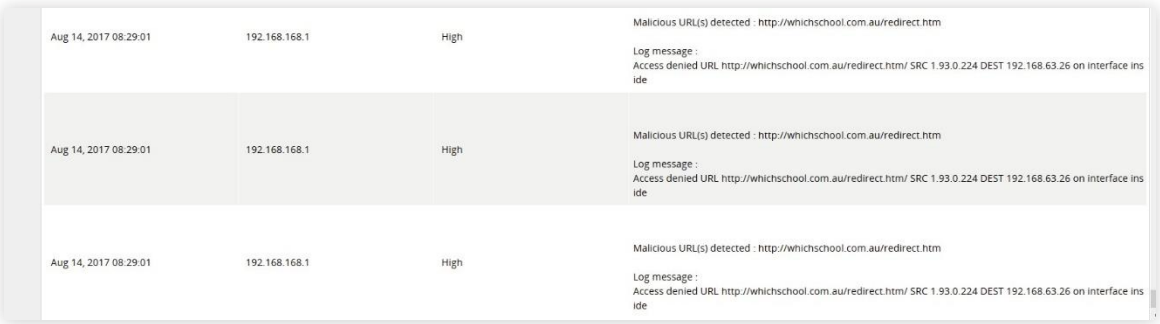
Você também pode editar, excluir ou gerenciar os feeds de ameaças adicionados na página de **Configurações** > **Gerenciamento de ameaças.**

Acessando notificações de alerta para a plataforma de inteligência contra ameaças do Log360

Todos os alertas disparados da plataforma de inteligência contra ameaças do Log360 podem ser encontrados em Alertas -> Alertas baseados em perfil -> Ameaças padrão.

Para alterar as configurações de notificação para esses perfis de alerta, clique no botão Gerenciar perfil de alerta ou no ícone de edição (✎).





O Log360 permite que você aproveite uma base de conhecimento global de ameaças e garante que nenhum intruso mal-intencionado possa invadir sua rede. Além dos alertas em tempo real, a solução também permite gerenciar os alertas como tickets, atribuindo proprietários, atualizando seus status e muito mais. Tudo isso não requer configuração adicional, então você pode adicionar uma camada extra de segurança sem nenhum esforço.