Funcionalidades técnicas do ESET Threat Intelligence

FEEDS DE DADOS EM TEMPO REAL

Os feeds de dados do ESET Threat Intelligence utilizam formato STIX/TAXII largamente suportados , que tornam fácil a integração com as ferramentas SIEM existentes. Esta integração ajuda a fortalecer os provedores de serviços e entrega as informações mais atualizadas sobre a imagem da ameaça para prever e prevenir as ameaças antes que elas ataquem. Atualmente, há três tipos principais de feeds disponíveis: Botnet, arquivo maliciosos e Feed de domínio. Todos os feeds que contenham novos metadados são atualizados a cada 5 minutos.

RELATÓRIOS COM ANTECEDÊNCIA

Fornece relatórios baseados nas combinações de regras do YARA sobre programas, atividiade ou configurações relacionadas que estejam sendo ou preparadas ou já utilizadas em um ataque contra uma empresa específica ou seu cliente.

API ROBUSTO

O ESET Threat Intelligence apresenta um API completo que está disponível para automatixação de relatórios, regras YARA e outras funcionalidades que permitam a integração com outros sistemas usados dentro das organizações.

ENVIO DE AMOSTRA DO ANDROID

Com o ESET Threat Intelligence é possível monitorar se o malware do Android está se direcionando para um aplicativo móvel corporativo. Isso é especificamente importante para bancos e outras indústrias que tem seus próprios aplicativos móveis. Adicionalmente, a qualquer momento uma empresa pode fazer upload de um aplicativo Android dentro do ESET Threat Intelligence para uma análise completa de um arquivo .apk.

REGRAS YARA

Permite às empresas configurar regras customizadas para obter informações específicas da empresa na qual os engenheiros de segurança estejam interessados. Uma vez que estas regras estejam configuradas, as empresas recebem detalhes valiosos como o número de vezes que eles foram vistos no mundo todo, URLs, códigos maliciosos contidos, comportamento de malware no sistema, onde foi detectado e mais.

ANÁLISE DE AMOSTRA AUTOMATIZADA

Cria uma relatório customizado baseado nos arquivos enviados ou hash, que fornece informações valiosas para decisões beseadas em fatos e investigações de incidentes.

ESET EM NÚMEROS

+ de 110
milhões de usuários no mundo todo.

+ de 400
mil clientes corporativos

+ de 200
países e territórios

13
centros globais de pesquisa e desenvolvimento

VISÃO GERAL

THREAT INTELLIGENCE

Aumente sua inteligência de segurança da rede local para o ciberespaço global

ENJOY SAFER TECHNOLOGY™

30 ANOS DE INOVAÇÃO CONTÍNUA EM SEGURANÇA

A diferença da ESET

EXPERTISE HUMANA APOIADA POR APRENDIZADO DE MÁQUINA

O uso de aprendizado de máquina para automatizar decisões e avaliar possíveis ameaças é uma parte vital de nossa abordagem. Mas ela é somente tão forte quanto as pessoas que ficam por trás do sistema. A expertise humana é primordial para fornecer a inteligência de ameaça mais precisa possível, já que aqueles que espalham as ameaças também são oponentes inteligentes.

SISTEMA DE REPUTAÇÃO

Os produtos para endpoint da ESET contém sistema de reputação na nuvem que se alimenta das informações relevantes sobre as ameaças mais recentes e arquivos benignos. Nossos sistema de reputação, o LiveGird, é feito de 110 milhões de sensores em todo o mundo e verificado por nossos centros de pesquisa e desenvolvimento, que dão aos clientes o mais alto nível de confiança quando visualizando informações e relatórios dentro de seu console.

PRESENÇA EM TODO O MUNDO

A ESET está na indústria de segurança há 30 anos, tem 22 escritórios em todo o mundo, 13 centros de pesquisa e desenvolvimento e a presença em mais de 200 países e territórios. Isso ajuda a fornecer aos clientes do mundo todo uma perspectiva das tendências e ameaças mais recentes.

Painel do ESET Threat Intelligence

Relatórios e feeds com antecedência

Relatórios

RELATÓRIO DE MALWARE DIRECIONADO

Mantém o usuário informado sobre um ataque potencial que esteja sendo preparado ou um ataque que já esteja acontecendo focado especificamente contra sua empresa. Este relatório inclui strings de regra YARA, informações sobre reputação, binários similares, detalhes de arquivos, produção de sandbox e mais.

RELATÓRIO DE ATIVIDADE DE BOTNET

Entrega dados regulares e quantitativos sobre famílias de malware identificadas e variantes de malware botnet. O relatório fornece dados acionáveis que incluem servidores de Comando e Controle (C&C) envolvidos em gerenciamento de botnet, amostras de botnet, estatísticas globais semanais e uma lista de alvos deste malware.

RELATÓRIO DE CERTIFICADO SSL FORJADO

Gerado quando a ESET detecta um certificado SSL lançado recentemente por uma autoridade de certificação que tenha um ativo muito similar àquele fornecido pelo cliente durante a configuração inicial. Isso pode incluir coisas como campanhas de phishing que ainda estejam por vir e que estejam tentando alavancar o certificado. Este relatório fornece atributos chave do certificado, combinações com o YARA e dados de certificado.

RELATÓRIO DE PHISHING DIRECIONADO

Mostra dados a respeito de todas as atividades de e-mail de phishing direcionadas na emrpesa selecionada. O relatório fornece informações cobre campanha de phishing que incluem tamanho da campanha, número de clientes, URL, screesnhots, prévia do e-mail de phishing, localização dos servidores e muito mais. de phishing, la ubicación de los servidores y mucho más.

Feeds

FEED DE BOTNET

Apresenta três tipos de feeds que checam mais de 1000 alvos por dia, incluindo informações sobre o próprio botnet, servidores envolvidos e seus alvos. Os dados fornecidos diretamente por estes feeds incluem itens como detecção, hash, data em que o servidor foi visto ativo pela última vez, arquivos baixados, endereços de IP, protocolos, alvos e muito mais.

FEED DE DOMÍNIO

Apresenta domínios que são considerados maliciosos, incluindo o nome do domínio, endereço de IP, detecção de arquivo baixado de uma URL e detecção de arquivo que estava tentando acessar a URL.

FEED DE ARQUIVO MALICIOSO

Apresenta executáveis que são considerados maliciosos e reconhece e compartilha as informações como SHA1, MD5, SHA256, detecção, tamanho e formato de arquivo.

FEEDS CUSTOMIZADOS

A ESET pode fornecer um feed completamente novo baseado em requisitos específicos da empresa. Além disso, todos os feeds atualmente disponíveis são ajustáveis de acordo com as necessidades dos clientes.

A disponibilidade dos informes e feeds do ESET Threat Intelligence varia de acordo com o país. Entre em contato com seu representante local da ESET para obter mais informações.