kaspersky bring on the future

Kaspersky Threat Intelligence

Kaspersky Threat Data Feeds

Visão geral

O que inclui?

As entradas de feeds fornecidos pela Kaspersky contêm dados contextuais que ajudam você a confirmar e priorizar ameaças com agilidade:

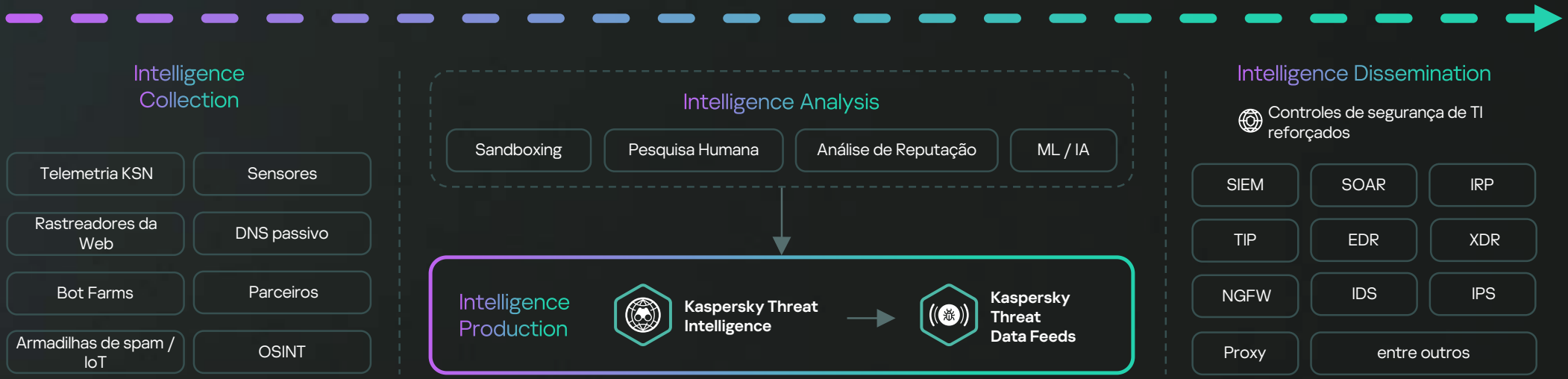
- nomes de ameaças
- endereços de IP e nomes de domínio de recursos maliciosos da Web
- hashes de arquivos maliciosos
- identificadores de objetos vulneráveis e comprometidos
- táticas, técnicas e procedimentos de ataques segundo a classificação MITRE AT&CK
- marcação de data e hora
- posição geográfica
- popularidade, e assim por diante...

O Kaspersky Threat Data Feed fornece informações de inteligência de ameaças em tempo real, para ajudar você a proteger suas redes e sistemas contra ciberameaças. Os feeds de dados incluem informações sobre malware conhecidos, sites de phishing, vulnerabilidades e exploits mais recentes, e outros tipos de ciberameaças. As empresas podem usar essas informações para bloquear tráfego malicioso, atualizar seus softwares de segurança e adotar outras medidas para se protegerem contra ciberataques.

Os dados são coletados de uma variedade de fontes confiáveis, incluindo o Kaspersky Security Network e nossos próprios rastreadores, serviços de monitoramento contra ameaças de botnets (rastreamento 24 horas de botnets e seus alvos), armadilhas de spam, dados de grupos de pesquisa, parceiros e muito mais.

Todas as informações coletadas são cuidadosamente verificadas e tratadas em tempo real, usando vários métodos de pré-processamento: sandboxing, análise estatística e investigativa, ferramentas comparativas, perfil comportamental e análise de especialistas.

Os feeds de dados ajudam a coletar informações sobre ameaças sobre um alerta ou incidente e a aprofundar os detalhes. Também ajuda a responder às perguntas sobre “Quem? O que? Onde? Por quê?” e a identificar a origem dos ataques, permitindo uma tomada de decisão rápida para proteger sua empresa contra ameaças de qualquer complexidade.



Como usar feeds de dados

Nome do feed	Prevenção	Detecção	Investigação
Feed de Dados de URL IoT	•	•	•
Feed de Dados de URL IoT	•	•	•
Feed de dados de URL de phishing	•	•	•
Feed de dados de URL de C&C Botnet	•	•	•
Feed de dados de URL de comando e controle de botnet móvel	•	•	•
Feed de dados de hash malicioso	•	•	•
Feed de dados de hash malicioso	•	•	•
Feed de dados de reputação de IP	•	•	•
Feed de Dados de URL IoT	•	•	•
Feed de Dados de Vulnerabilidade	•	•	•
Feed de dados de vulnerabilidade ICS	•	•	•
ICS Vulnerability Data Feed em formato OVAL		•	
Feed de Dados de Hash ICS	•	•	•
Feed de dados pDNS			•

Nome do feed	Prevenção	Detecção	Investigação
Feed de dados de Regras Suricata		•	
Feed de dados do Kaspersky Cloud Access Security Broker (CASB)		•	
Feed de dados de hash APT		•	•
Feed de dados de APT IP		•	•
Feed de dados de APT URL		•	•
Feed de dados APT Yara		•	•
Feed de dados de ameaças de software de código aberto	•	•	•
Feed de Dados de Hash de Cibercrimes		•	•
Feed de Dados de URL Crimeware			•
Feed de dados Yara de Crimeware			•
Feed de Dados Regras Sigma	•		
Feed de Dados IP de Segurança de Rede	•	•	
Feed de Dados de URL de Segurança de Rede	•	•	
Feed de dados de Filtragem da Web de Segurança de Rede	•	•	

A lista de Feeds de Dados de Ameaças da Kaspersky está constantemente se expandindo.

Descrição dos Feeds de Dados de Ameaças da Kaspersky

Feeds comerciais

Os feeds comerciais fornecem acesso à coleção mais abrangente de informações disponíveis por assinatura. As informações são atualizadas regularmente. Dependendo do tipo de feed, a regularidade das atualizações pode variar de alguns minutos a várias horas. Além dos feeds de dados listados, você pode solicitar a criação de um feed personalizado adaptado às suas necessidades.

Nome do feed	Descrição do feed	Tipo de indicador	Casos de uso
Feed de Dados de URL IoT	Recursos da web a partir dos quais o malware é distribuído	Máscara de Rede	• Os sistemas de gestão de segurança da informação estão abertos para enriquecimento com fontes externas de informação. Conectar esses fluxos ao SIEM / SOAR / IRP permite que os usuários respondam às ameaças atuais de forma oportuna e criem contexto adicional ao investigar um incidente. • A integração com sistemas de segurança de rede e de e-mail (por exemplo, NGFW / IDS / IPS / Mail / Web Security) ajuda a prevenir incidentes cibernéticos por meio do enriquecimento das capacidades de controle de segurança nativas com IOCs provenientes de feeds de dados.
Feed de Dados de URL IoT	Recursos da web pelos quais o ransomware é distribuído		
Feed de dados de URL de phishing	Recursos de Phishing da Web		
Feed de dados de URL de C&C Botnet	Servidores de comando e controle de botnets e objetos maliciosos relacionados (bots)		
Feed de dados de URL de comando e controle de botnet móvel	Servidores de botnet móvel C&C com objetos maliciosos associados (bots)		

#prevenção

#detecção

#investigação

Nome do feed	Descrição do feed	Tipo de indicador	Casos de uso	
Feed de dados de hash malicioso	Hashes de arquivos maliciosos comuns	Hash	• Integração com sistemas de segurança de infraestrutura (Segurança de Endpoint, Segurança de Servidor, Segurança de Email/Web) para evitar que malware seja baixado e executado, bem como detectar malware que já está em execução. • A integração com sistemas SIEM / SOAR / IRP permite que os usuários respondam rapidamente às ameaças atuais e criem contexto adicional ao investigar um incidente.	#prevenção #detecção #investigação
Feed de dados de hash malicioso	Hashes de arquivos maliciosos comuns para sistemas operacionais móveis (Android e iOS)			
Feed de dados de reputação de IP	Várias categorias de endereços IP suspeitos e maliciosos	IP	• A integração com sistemas de segurança de rede e de e-mail (NGFW / Segurança de E-mail) ajuda a prevenir incidentes cibernéticos ao complementar o banco de dados nativo de indicadores de comprometimento com dados sobre ameaças atuais. • A integração com sistemas de classe SIEM/ SOAR/IRP permite que os usuários respondam rapidamente às ameaças atuais e criem contexto adicional ao investigar um incidente.	#prevenção #detecção #investigação
Feed de Dados de URL IoT	Recursos da web que distribuem software malicioso para dispositivos IoT (câmeras IP, aspiradores inteligentes, bules elétricos, cafeteiras etc.)	Máscara de Rede		
Feed de Dados de Vulnerabilidade	Vulnerabilidades de software empresarial	CVE	• Identificação de elementos de infraestrutura vulneráveis por meio da integração com scanners de vulnerabilidade e sistemas de Gerenciamento de Ativos. • Integração com sistemas de Proteção de Endpoint para prevenir o lançamento de software contendo vulnerabilidades críticas. • Detecção do lançamento de software vulnerável. • Assistência com investigações. • Recomendações para mitigação de vulnerabilidades.	#prevenção #detecção #investigação
Feed de dados de vulnerabilidade ICS	Vulnerabilidades em software e hardware de ICS, bem como em software corporativo usado na infraestrutura de controle de processos.			

Nome do feed	Descrição do feed	Tipo de indicador	Casos de uso	
ICS Vulnerability Data Feed em formato OVAL	Regras para buscas automatizadas de vulnerabilidades de software ICS	Verificação OVAL	• Enriquecimento de scanners de vulnerabilidades de software populares para detectar software de ICS vulnerável.	#detecção
Feed de Dados de Hash ICS	Arquivos maliciosos comuns que representam uma ameaça para os sistemas de controle industrial (ICS)	Hash	• Na periferia das redes OT, semelhante aos cenários de uso do Malicious Hash Data Feed. • Dentro das redes OT para detectar arquivos potencialmente perigosos.	#prevenção #detecção #investigação
Feed de dados pDNS	Registros de consultas DNS para domínios e seus respectivos endereços IP ao longo de um período	IP, FQDN	• Fornecendo contexto ao investigar incidentes cibernéticos	#investigação
Feed de dados de Regras Suricata	Regras para detectar várias categorias de ameaças no tráfego de rede, como APT, Botnet C&C, Ransomware etc.	Regras Suricata	• Integração com sistemas NGFW/IDS/IPS/NTA/ NDR para enriquecer as regras de detecção de atividades maliciosas.	#detecção
Feed de dados do Kaspersky Cloud Access Security Broker (CASB)	Domínios e hosts relacionados a serviços de nuvem populares	Máscara de Rede	• Construindo uma solução CASB, em particular, para configurar políticas de acesso para serviços em nuvem.	#detecção

Nome do feed	Descrição do feed	Tipo de indicador	Casos de uso	
Feed de dados de hash APT	Hashes de arquivos usados por gangues da APT para realizar ataques direcionados	Hash	• Integração com sistemas de segurança de infraestrutura (Segurança de Endpoint e Servidor) para evitar que malware seja baixado e executado, bem como detectar malware que já está em execução. • A integração com sistemas de segurança de rede e de e-mail (por exemplo, NGFW / IDS / IPS / Mail / Web Security) ajuda a prevenir incidentes cibernéticos por meio do enriquecimento das capacidades de controle de segurança nativas com IOCs provenientes de feeds de dados. • A integração com sistemas de classe SIEM / SOAR / IRP permite aos usuários criar contexto adicional ao investigar um incidente, bem como responder prontamente a ameaças atuais relacionadas a ataques direcionados ou a membros de grupos APT.	#detecção #investigação
Feed de dados de APT IP	Informações sobre elementos de infraestrutura relevantes para a realização de ataques direcionados.	IP		
Feed de dados de APT URL		Máscara de Rede		
Feed de dados APT Yara	Regras YARA para identificar arquivos usados em ataques direcionados	Regras YARA	• Busca proativa por sinais de ataques direcionados na infraestrutura de uma organização. • Útil ao investigar incidentes cibernéticos.	#detecção #investigação
Feed de dados de ameaças de software de código aberto	Pacotes de software de código aberto contendo vulnerabilidades, funcionalidades maliciosas ou comprometimentos de funcionalidade politicamente motivados (bloqueio em certas regiões, slogans políticos etc.).	Nome e versão do produto	• Projetado para análise de componentes de software desenvolvido como parte do processo de desenvolvimento seguro (DevSecOps) a fim de proteger o software de ataques à cadeia de suprimentos, detectar e eliminar precocemente vulnerabilidades, e prevenir o uso de pacotes contendo recursos politicamente orientados não declarados (NDV).	#prevenção #detecção #investigação

Nome do feed	Descrição do feed	Tipo de indicador	Casos de uso	
Feed de Dados de Hash de Cibercrimes	Hashes de arquivos usados em campanhas fraudulentas descritas nos relatórios de Crimeware da Kaspersky.	Hash	• Detecção de atividade maliciosa associada às ações fraudulentas de intrusos. • Ajude na resolução do incidente fornecendo informações adicionais contidas nos feeds de dados de ameaças.	#detecção #investigação
Feed de Dados de URL Crimeware	Informações sobre elementos de infraestrutura relacionados a campanhas fraudulentas descritas nos relatórios de crimeware da Kaspersky.	Máscara de Rede		
Feed de dados Yara de Crimeware	Regras YARA para identificar arquivos usados em campanhas fraudulentas descritas nos relatórios de crimeware da Kaspersky.	Regras YARA	• Procure antecipadamente sinais de campanhas fraudulentas na infraestrutura da organização. • Útil ao investigar incidentes cibernéticos.	#investigação
Feed de Dados Regras Sigma	Regras em formato YAML para detectar atividades maliciosas	Regras da SIGMA	• Integração com SIEM/EDR para detectar atividades maliciosas.	#detecção
Feed de Dados IP de Segurança de Rede	Lista de endereços IP para listas de alerta/negação de NGFW	IP	• Integração com controles de segurança de rede (NGFWs) para aumentar seu nível de proteção	#detecção #prevenção

Nome do feed	Descrição do feed	Tipo de indicador	Casos de uso	
Feed de Dados de URL de Segurança de Rede	Lista de URLs para listas de alerta/negação de NGFW	URL	• Integração com controles de segurança de rede (NGFWs) para aumentar seu nível de proteção	#detecção #prevenção
Feed de dados de Filtragem da Web de Segurança de Rede	Lista de domínios categorizados para listas de alerta/negação de NGFW	URL	• Integração com controles de segurança de rede (NGFWs) para aumentar seu nível de proteção	#detecção #prevenção

Demo de feeds

Os feeds de demonstração são apenas para fins de avaliação. Os dados contêm amostras limitadas com informações significativamente reduzidas e atualizações menos frequentes.
A estrutura dos feeds é semelhante ao formato dos feeds comerciais, mas isso pode diferir em alguns casos.

- Feed de dados de reputação de IP Demo
- Feed de dados de URL de C&C Botnet Demo
- Feed de dados de hash malicioso Demo
- Feed de dados de APT IP Demo
- Feed de dados de APT URL Demo
- Feed de dados de Regras Sigma
- Feed de dados de hash APT Demo
- Feed de dados de Regras Suricata Demo
- Feed de dados de Regras Suricata Demo
- Feed de dados Kaspersky ICS Vulnerability Demo
- Feed de Dados de Vulnerabilidade Demo ICS no formato OVAL
- Feed de Dados de Hash de Crimeware Demo
- Feed de dados de Crimeware URL

Solicite uma demo

Kaspersky Threat Intelligence

Seu rico suporte contexto

O Threat Data Feeds da Kaspersky aprimora os recursos de detecção de seus controles de segurança existentes, incluindo sistemas SIEM, sistemas de detecção de intrusão, proxies de segurança etc.

Saiba mais

www.kaspersky.com.br