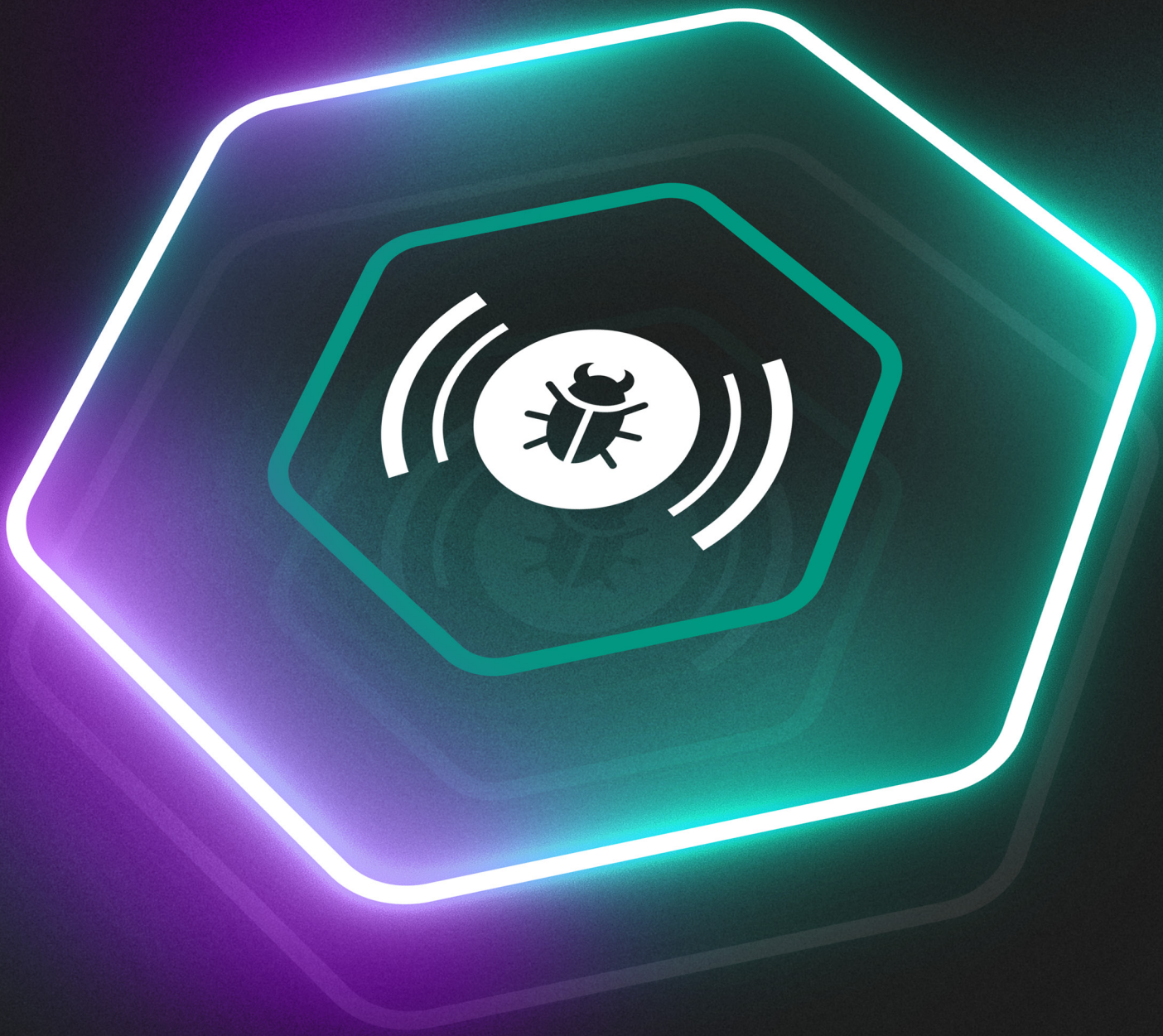


Kaspersky Threat Data Feeds

kaspersky PREPARADOS PARA O FUTURO

Kaspersky Threat Data Feeds

Os ciberataques acontecem todos os dias. As ameaças virtuais estão em constante crescimento em termos de frequência, complexidade e ofuscação, à medida que tentam comprometer suas defesas. Os adversários utilizam cadeias de destruição, campanhas e táticas, técnicas e procedimentos (TTPs) personalizados de intrusão complicadas para perturbar seu negócio ou causar danos aos seus clientes. É notório que a proteção exige novos métodos, baseados em inteligência de ameaças.

Ao integrar feeds de inteligência de ameaças sempre atualizados contendo informação sobre IPs, URLs e hashes de arquivos suspeitos e perigosos nos sistemas de segurança existentes, como SIEM, SOAR e plataformas de inteligência de ameaças, as equipes de segurança podem automatizar o processo de triagem de alertas inicial, fornecendo simultaneamente aos seus especialistas em triagem contexto suficiente para identificar imediatamente alertas que devem ser investigados ou encaminhados para equipes de resposta a incidentes para investigação e resposta adicionais.

- FEED DE REPUTAÇÃO DE IP
- FEED DE HASH (WIN/*nix/ MacOS/AndroidOS/ iOS)
- FEEDS DE URL (Maliciosos, Phishing e C&C)
- FEED DE URL DE RANSOMWARE
- FEEDS DE IOC APT
- FEED DE VULNERABILIDADE
- FEED DE DNS PASSIVO (pDNS)
- FEED DE URL DE IoT
- FEED DE LISTA DE PERMISSÕES
- FEED DE HASH ICS
- E MUITO MAIS

Kaspersky Threat Data Feeds

Dados contextuais

Cada registro em cada feed de dados é enriquecido também com contextos acionáveis (nomes das ameaças, carimbos de data/hora, geolocalização, endereços IP solucionados de recursos infectados da web, hashes, popularidade, etc.). Os dados contextuais ajudam a mostrar um panorama geral para uma maior validação e suporte da utilização abrangente dos dados. Fornecidos com contexto, os dados podem ser usados diretamente para responder perguntas do tipo "quem, o quê, onde, quando" para identificar seus adversários e ajudar você a tomar decisões rápidas para agir.

Destaques

Os feeds de dados são automaticamente gerados em tempo real, com base em descobertas em todo o mundo (o Kaspersky Security Network fornece visibilidade a uma porcentagem significativa de todo o tráfego da Internet, abrangendo dezenas de milhões de usuários finais em mais de 213 países), fornecendo altas taxas de detecção e precisão

Facilidade de implementação. Documentação adicional, amostras, um gerente de conta técnico dedicado e suporte técnico da Kaspersky combinam-se para permitir uma integração direta.

Centenas de especialistas, incluindo analistas de segurança de todo o mundo, especialistas em segurança de renome mundial das equipes GReAT e R&D contribuem para gerar esses feeds. Os agentes de segurança recebem informações críticas e alertas gerados a partir de dados da mais alta qualidade, sem correr o risco de serem inundados por indicadores e avisos supérfluos

Coleta e processamento

Os Feeds de Dados são montados a partir de fontes fundidas, heterogêneas e altamente confiáveis, tal como o Kaspersky Security Network e os nossos próprios Web Crawlers, o serviço Botnet Monitoring (monitoramento 24 horas por dia, 7 dias da semana, 365 dias do ano de botnets e seus alvos e atividades), armadilhas de spam, equipes de pesquisa e parceiros.

Em seguida, em tempo real, todos os dados agregados são analisados detalhadamente e refinados através de várias técnicas de pré-processamento, como critérios estatísticos, sandboxes, análise heurística, ferramentas de semelhança, profiling comportamental, validação por analistas e verificação em listas de permissões.

Formatos de disseminação leves e simples (JSON, CSV, OpenIoC, STIX) por meio de HTTPS, TAXII ou mecanismos de ad-hoc delivery, suportam fácil integração de feeds em soluções de segurança

Todos os feeds são gerados e monitorados por uma infraestrutura com elevada tolerância a falhas, assegurando disponibilidade contínua

Feeds de dados repletos de falsos positivos não têm valor, por isso, são aplicados testes e filtros muito extensos antes de lançar os feeds, para garantir que 100% dos dados verificados sejam entregues

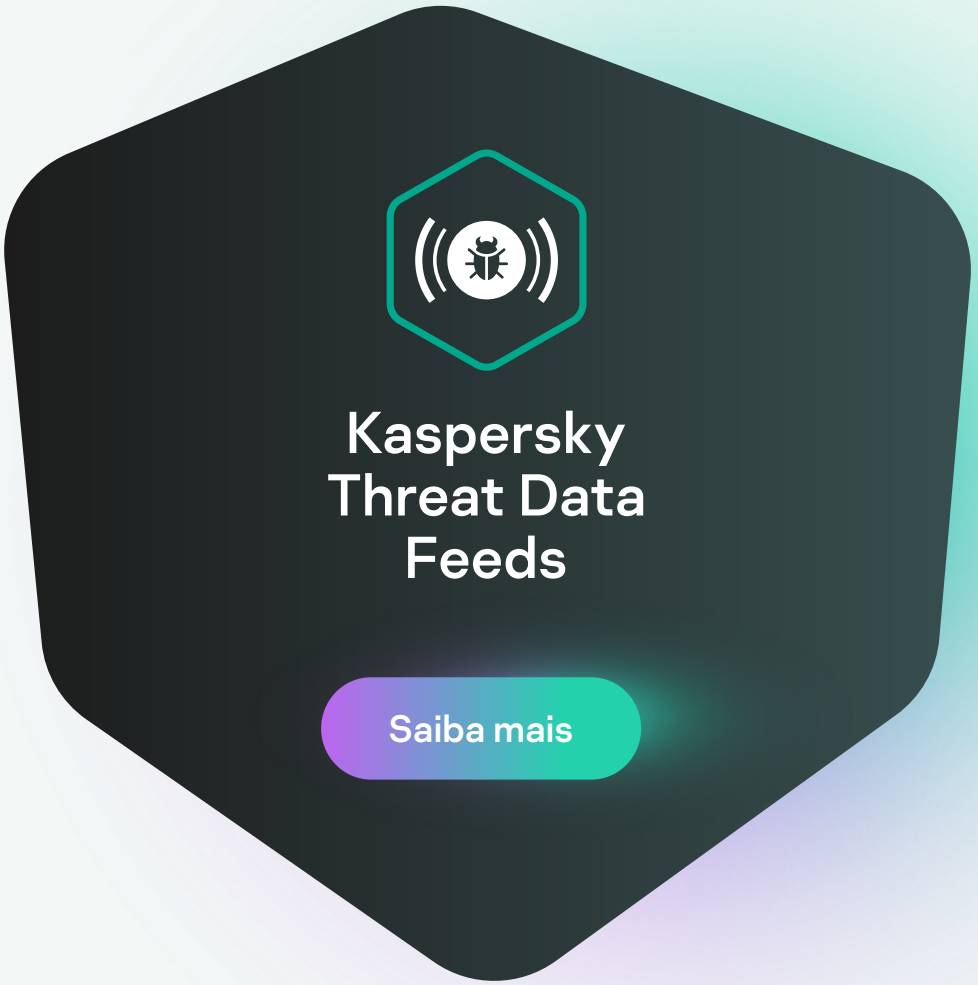
Benefícios

Reforce suas soluções de defesa de rede, incluindo SIEMs, firewalls, IPS/IDS, proxy de segurança, soluções de DNS, anti-APT, com indicadores de comprometimento (IOCs) atualizados continuamente, e contexto acionável para fornecer insights sobre ciber ataques e uma maior compreensão da intenção, das capacidades e dos alvos dos seus adversários. Os principais SIEMs (incluindo HP ArcSight, IBM QRadar, Splunk etc.) e plataformas de TI são totalmente suportados

Melhore e acelere sua resposta a incidentes e capacidades forenses automatizando o processo de triagem inicial, ao mesmo tempo em que fornece aos analistas de segurança contexto suficiente para identificar imediatamente alertas que precisam ser investigados ou escalados para equipes de resposta a incidentes para investigação e resposta adicionais

Impeça o roubo de ativos confidenciais e propriedade intelectual de máquinas infectadas para fora da organização. Detecte ativos infectados rapidamente para proteger a reputação da sua marca, manter sua vantagem competitiva e garantir oportunidades de negócios

Sendo um MSSP, expanda seu negócio fornecendo uma inteligência de ameaças líder no setor como serviço premium aos seus clientes. Sendo uma CERT, melhore e expanda suas capacidades de detecção e identificação de ciberameaças



www.kaspersky.com.br