Kaspersky Threat Intelligence

Esteja a frente de seus adversários

kaspersky

Fontes do Kaspersky Threat Intelligence

A Kaspersky Threat Intelligence fornece acesso a uma ampla gama de informações coletadas por nossos analistas e pesquisadores que estão entre os melhores do mundo para ajudar sua organização a combater efetivamente as ameaças cibernéticas de hoje.

Inteligência de ameaças impulsionada por expertise e conhecimento global exclusivos

Cada centro contribui para as soluções e serviços da Kaspersky.

- Pesquisa sobre ameaças
- Investigação de Incidentes

Kaspersky Global Equipe de pesquisa e análise de fraudes

- Pesquisa das ameaças mais complexas: APT, campanhas de espionagem cibernética, epidemias cibernéticas globais etc.
- Segurança das tecnologias voltadas para
- Investigação de crimes cibernéticos financeiros sofisticados

Kaspersky Pesquisa sobre ameaças

- Pesquisa antimalware
- Pesquisa de filtragem de conteúdo
- Metodologias SSDLC e Secure-by-Design

Kaspersky Pesquisa sobre tecnologias de IA

- Cibersegurança de IA
- Pesquisa de GenAI
- Detecção/soluções de ameaças com IA

Kaspersky Serviços de segurança

- MDR
- Incident Response
- Security Assessment
- Consultoria em SOC
- Digital Footprint Intelligence

Kaspersky ICS CERT

- Análise de ameaças à infraestrutura crítica
- Pesquisa e avaliação de vulnerabilidades do ICS
- Associações, análises e padrões de tecnologia

Destaques do Kaspersky Threat Intelligence

Nosso profundo conhecimento, extensa experiência em pesquisa de ameaças cibernéticas e insights únicos em todos os aspectos da cibersegurança nos tornaram um parceiro confiável para empresas em todo o mundo e um aliado valorizado para as forças policiais e organizações governamentais, incluindo a Interpol e numerosas unidades CERT.

Cobertura de ameaças globais, com vasta experiência em pesquisar ameaças em regiões de onde a maioria dos ataques se originam

Contribuição contínua dos especialistas da Kaspersky

Inteligência de ameaças para os segmentos de TI e TO

Destaques do Kaspersky Threat Intelligence

Nós rastreamos:

Mais de 300

agentes de ameaças

Mais de 500

campanhas

Mais de 200

relatórios privados produzidos por ano

170000+

IoCs relacionados a relatórios

2 500+

Regras YARA relacionadas a relatórios

Níveis de dados de inteligência de ameaças

Tático

Informações de baixo nível altamente perecíveis que apoiam operações de segurança e resposta a incidentes. Um exemplo de inteligência tática são os IOCs relacionados a um comportamento de um ataque recém-descoberto.

Funções:

- Analista do SOC

Sistemas:

- SIEM
- NGFW
- SOAR
- IPS
- IDS

Processos:

- Busca de ameaças
- Monitoramento

Operacional

Este nível geralmente inclui dados sobre campanhas e TTPs de ordem superior. Pode incluir informações sobre a atribuição específica de atores, bem como as capacidades e intenções dos adversários.

Funções:

- SOC L3 Analyst
- Analista de DFIR
- Analista de IR

Sistemas:

- SIEM
- NTA
- TIP
- EDR / XDR

Processos:

- Incident Response
- Busca de ameaças

Estratégico

Este nível oferece suporte aos executivos de nível C e aos conselhos de administração na tomada de decisões importantes sobre avaliações de risco, alocação de recursos e estratégia organizacional. Esta informação inclui tendências, motivações dos atores e suas classificações.

Funções:

- CISO
- CTO
- CIO
- CEO

Processos:

- Construindo uma estratégia de SI
- Conscientização

Formatos de entrega de inteligência de ameaças

Inteligência de Ameaças legível por máquina

Kaspersky Threat Data Feeds

30+ feeds de dados de ameaças que atendem a diferentes necessidades, com cobertura de TI e TO e plataforma de inteligência de ameaças.

Inteligência de ameaças legível por pessoas

Kaspersky Threat Intelligence Portal

O portfólio principal da Kaspersky Threat Intelligence para ambientes de TI e TO com um único ponto de acesso via Portal do Kaspersky Threat Intelligence.

Suporte especializado do Threat Intelligence

Kaspersky Takedown Service

Kaspersky Ask the Analyst

Orientação especializada de profissionais experientes

Kaspersky Threat Intelligence

Kaspersky Threat Data Feeds

Mais de 30 fontes de dados de ameaças inovadoras para diferentes tarefas.

Fontes de dados de ameaças personalizadas para sua organização também estão

- Ti tática
- TI operacional

Feeds de dados de ameaças gerais

- URLs maliciosos
- URL de Ransomware
- URLs de phishing
- URLs de botnet C&C
- Botnet em Dispositivos Móveis C&C URL
- Hashes maliciosos
- Hashes maliciosos em dispositivos móveis
- Reputação de IP
- IoT URL
- ICS Hashes
- APT Hashes
- IP APT
- URL APT
- Hashes de crimeware
- Ciberware de URL

Kaspersky Threat Data Feeds → SIEM, SOAR / IRP, TIP, EDR / XDR

Plataforma de TI

Operacionalize rapidamente suas várias fontes de inteligência de ameaças e reduza a carga de trabalho dos SIEMs.

Kaspersky CyberTrace

Feeds de dados de ameaças específicas

Feed de dados de segurança de rede	Feed de regras Suricata	Feed de Dados Regras Sigma	Feeds de dados de regras de Yara	Feed de vulnerabilidades	Feed de dados de ameaças de software de código aberto
NGFW	IDS / IPS	SIEM / EDR	YARA-scanner	SBOM / CMDB	OSA / CSA / ASOC

Kaspersky Threat Intelligence Portal

Um único ponto de acesso para o Kaspersky Threat Intelligence dentro de uma interface unificada / API, onde os serviços trabalham juntos, enriquecendo e reforçando uns aos outros. Reunindo toda a expertise e conhecimento da Kaspersky sobre ameaças cibernéticas em um só lugar, permite monitorar ameaças relevantes para uma organização específica usando tecnologias proprietárias de processamento e normalização de dados, e possibilita a análise de amostras de malware e sua atribuição.

- TI tática
- TI operacional
- TI estratégica

Kaspersky Threat Intelligence Portal versão gratuita

Panorama de Ameaças no Portal do Kaspersky Threat Intelligence

Inteligência de ameaças específicas da região e da indústria para entender as ameaças exatas enfrentadas pela sua organização.

- Alinhamento MITRE ATT&CK TTPs
- Atualizações em tempo real com base nas pesquisas em andamento da Kaspersky
- Preenchimento automático de perfis de adversários e software
- Repositório de regras de detecção

400 000+

Arquivos maliciosos que detectamos diariamente

Threat Landscape — como funciona

Suporte especialista do Kaspersky Threat Intelligence

Kaspersky Ask the Analyst

- TI operacional
- TI estratégica

O serviço Kaspersky Ask the Analyst amplia nosso Portfólio de Inteligência permitindo que você solicite orientação e informações sobre ameaças específicas que está enfrentando ou nas quais está interessado.

Nós capacitamos você com acesso a um grupo central de pesquisadores da Kaspersky caso a caso. O serviço oferece uma comunicação abrangente entre os especialistas, para aumentar suas capacidades existentes com nosso conhecimento e recursos exclusivos.

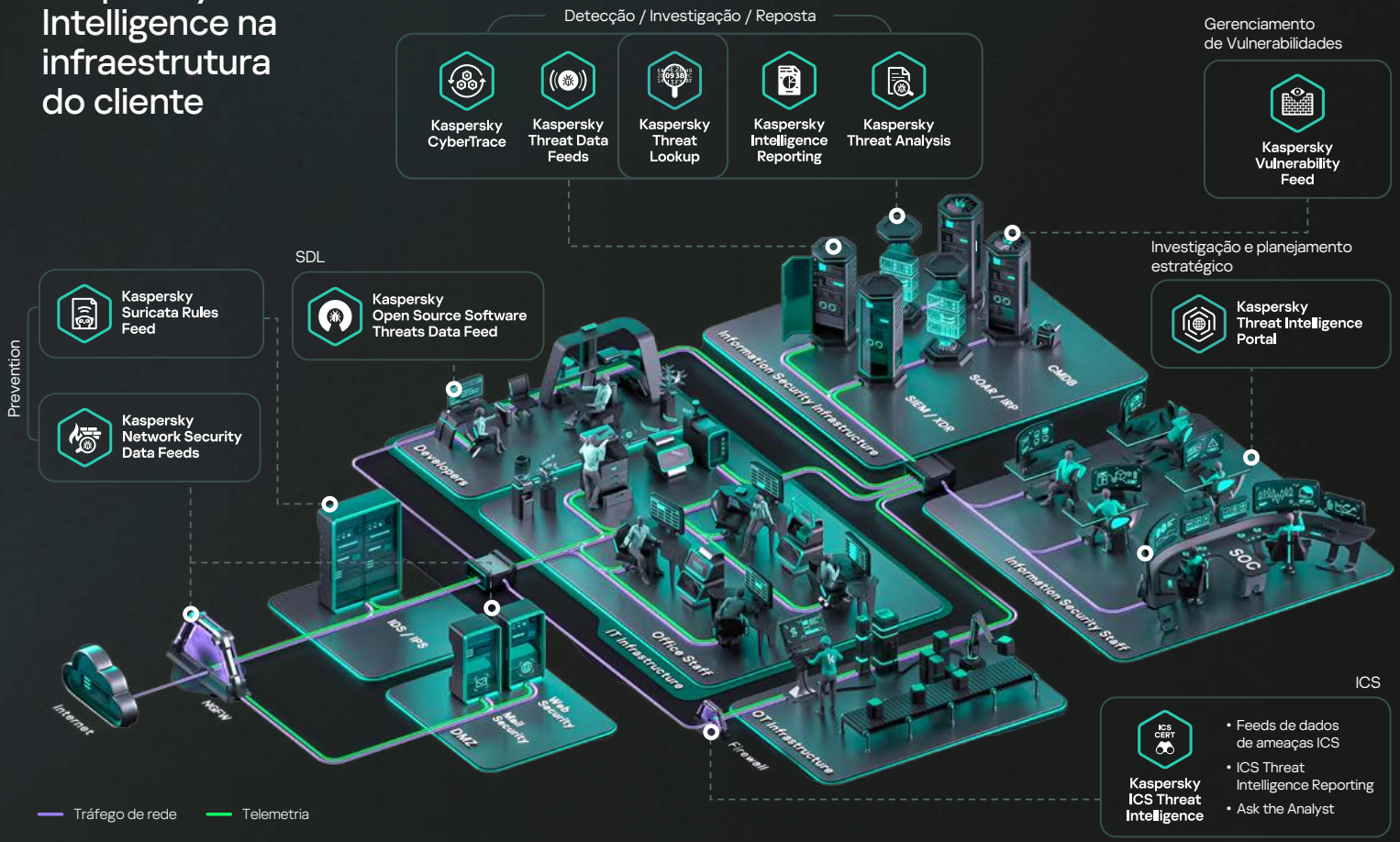
Kaspersky Takedown Service

- TI operacional

O Kaspersky Takedown Service mitiga rapidamente as ameaças representadas por domínios de phishing maliciosos antes que possam causar danos ao seu negócio e marca. Com ampla experiência em analisar domínios, sabemos como reunir todas as evidências necessárias para provar que são maliciosos. Vou cuidar da gestão de remoção para você.

O serviço é prestado globalmente em cooperação com organizações internacionais e agências de aplicação da lei nacionais e regionais.

Exemplo de Kaspersky Threat Intelligence na infraestrutura do cliente



Oferta Kaspersky Threat Intelligence Industrial

Inteligência de Ameaças legível por máquina

Kaspersky Threat Data Feeds

Dados legíveis por máquina sobre ameaças e vulnerabilidades de cibersegurança industrial:

Kaspersky ICS Hashes Data Feed
Kaspersky ICS Vulnerability Data Feed
Kaspersky ICS Vulnerability Data Feed em formato OVAL

Inteligência de ameaças legível por pessoas

Kaspersky ICS Intelligence Reporting

Acesse publicações regulares que abordam ameaças e vulnerabilidades de cibersegurança industrial no Portal do Kaspersky Threat Intelligence.

Suporte de especialistas de Threat Intelligence

Kaspersky Ask the Analyst

Consulte diretamente os especialistas da Kaspersky ICS CERT para obter conselhos personalizados sobre ameaças e vulnerabilidades de cibersegurança industrial, estatísticas de ameaças, panorama de ameaças, padrões do setor e muito mais.

Tático TI operacional TI estratégica

Por que escolher Kaspersky Threat Intelligence

Um principal provedor de TI reconhecido por analistas do setor.	Verificado por analistas de várias empresas globais de pesquisa, como Frost & Sullivan, Quadrant Knowledge Solutions, Forrester, IDC etc.
Múltiplas fontes confiáveis e únicas são utilizadas para produzir a TI confiável.	Nossa infraestrutura Kaspersky Security Network cobre +100M sensores em 200 países, os maiores repositórios de arquivos maliciosos e legítimos, Dark Web, atividades contínuas de TH e IR, rastreadores da web, armadilhas de spam etc.
Pessoas renomadas especializadas em TI e TO	200+ especialistas certificados de 5 centros de expertise, incluindo a equipe GReAT e ICS-CERT, distribuídos pelo mundo, falando mais de 20 idiomas. Os especialistas da Kaspersky estão sempre entre os primeiros a descobrir as ameaças mais notórias — desde Stuxnet e WannaCry até a Operation Triangulation.
Presença global	Uma forte presença nas regiões de onde a maioria dos ataques se originam (Rússia, CEI, China etc.) nos dá a capacidade única de coletar, analisar e distribuir inteligência de ameaças 100% verificada para organizações em qualquer país.
Experiência única em tecnologias de detecção de malware.	Como o maior fornecedor de AV (com os produtos mais premiados), processamos milhões de novas amostras de malware todos os dias, utilizando nossas tecnologias proprietárias de detecção de ameaças.
Experiência única em pesquisa de APT	Nós rastreamos centenas de atores e campanhas de APT, lançamos mais de 200 relatórios estratégicos detalhados anualmente e possuímos a maior coleção de arquivos de APT na indústria, que inclui mais de 70 mil amostras.
Alimentado por IA para aprimorar a detecção, resposta e relatório de ameaças	IA / ML nos permite extrair insights acionáveis, gerar relatórios personalizados e automatizar a análise, economizando tempo e recursos significativos.
Fornecedor robusto e seguro	Infraestrutura tolerante a falhas, transparente com alta SLA e capacidades de monitoramento, construída usando metodologias SDLC, com avaliações independentes regulares de terceiros (SOC 2 Type 2 ou ISO 27001).

Casos de sucesso

Isso nos dá uma ótima visibilidade das ameaças que nossos clientes estão enfrentando. Quando ocorre um alerta, ter informações autorizadas e referenciáveis, juntamente com todos os dados colaterais que você obtém com ele, é vital para construir uma imagem completa do que está acontecendo e do que podemos aprender com isso.

Paul Colwell
CyberGuard Technologies

CyberGuard Technologies

Leia a história

A Kaspersky costuma ser a primeira a identificar quando uma nova ameaça está surgindo, muitas vezes antes mesmo de os fabricantes de software saberem algo a respeito.

A Kaspersky tem a expertise para me informar sobre novas ameaças, o que está espreitando nas sombras e que desconhecemos, em vez de simplesmente me dar uma enxurrada de notícias recicladas que não acrescentam nada novo ao nosso entendimento.

Juan Andres Guerrero Saade
Pesquisador, Chronicle Security

chronicle

Leia a história

A Kaspersky superou as minhas expectativas com seus recursos e ouvindo o que precisávamos. Eles nos deram confiança no produto e nas pessoas por trás dele e nos permitiram ter uma rede mais segura.

Rashid AlNahlawi
Consultor de segurança de TI, Comitê Olímpico do Catar

قطر
QATAR

Leia a história

Kaspersky Threat Intelligence lhe dá a chance de...

Identificar e previnir proativamente ameaças.

O Kaspersky Threat Intelligence mantém você informado sobre as últimas ameaças e vulnerabilidades, capacitando-o a tomar medidas proativas para proteger seus sistemas antes que ocorra um ataque.

Aprimorar suas capacidades de detecção de ameaças .

O Kaspersky Threat Intelligence ajuda a complementar suas soluções de segurança existentes com as últimas informações sobre ameaças, melhorando sua capacidade de detectar e bloquear ameaças avançadas.

Melhorar sua resposta de incidente

O Kaspersky Threat Intelligence fornece informações em tempo real sobre ameaças emergentes e indicadores de comprometimento. Assim, você pode responder a incidentes de forma rápida e eficaz.

Obter visibilidade da sua pegada digital.

O Kaspersky Threat Intelligence fornece uma visão abrangente da sua pegada digital, incluindo todos seus bens digitais que podem estar vulneráveis a ataques ou a comprometimentos.

Enriquecer sua expertise interna

A equipe de especialistas da Kaspersky está entre os pesquisadores mais experientes e respeitados do setor, trazendo uma riqueza de conhecimento e expertise para as equipes de Segurança da Informação.

Cumprir regulamentos e normas

Todas as empresas estão sujeitas a diversas regulamentações e normas do seu setor de atuação. O Kaspersky Threat Intelligence auxilia na conformidade, ajudando você a cumprir com esses requisitos.

Muito obrigado(a)!

The Kaspersky Threat Intelligence Portal – o centro de conhecimento em cibersegurança

Kaspersky Threat Intelligence Portal

Saiba mais

Solicite uma demo