Esteja a frente de seus adversários

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky
Threat Intelligence

Kaspersky Threat Intelligence

A solução de Threat Intelligence da Kaspersky oferece acesso às informações de que você precisa para mitigar ciberameaças, além de obter informações relevantes para você, fornecidas pela nossa equipe líder mundial de investigadores e analistas.

O conhecimento, a experiência e as informações detalhadas da Kaspersky sobre todos os aspectos da segurança virtual fizeram com que nos tornássemos o parceiro de confiança das principais autoridades policiais e governamentais do mundo, incluindo a INTERPOL e as principais CERTs. O Kaspersky Threat Intelligence oferece acesso instantâneo a inteligência de ameaças, tática, operacional e estratégica.

O Kaspersky Threat Intelligence oferece uma visão abrangente do cenário global de ameaças. A solução combina fontes de inteligência, feeds de dados sobre ameaças e pesquisas internas, tudo analisado pela nossa equipe de especialistas para fornecer insights acionáveis que ajudam as organizações a se protegerem contra as ciberameaças.

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
- IPS
- IDS
- SOAR

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
- EDR/XDR
- TIP

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

Kaspersky Threat Intelligenceesquema do aplicativo

O Kaspersky Threat Intelligence capacita você a

Identificar e prevenir ameaças de forma proativa

O Kaspersky Threat Intelligence mantém você a par de tudo sobre as ameaças e vulnerabilidades mais recentes, permitindo adotar medidas proativas para proteger seus sistemas antes que ocorra um ataque.

Obter visibilidade sobre 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.

Aprimorar seus recursos de detecção de ameaças

O Kaspersky Threat Intelligence ajuda a reforçar as suas soluções de segurança implementadas com a mais recente inteligência de ameaças, aprimorando sua capacidade de detectar e bloquear ameaças avançadas.

Melhorar sua resposta a incidentes

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.

Cumprir com os 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.

Valorizar ainda mais seus especialistas internos

A equipe de especialistas Kaspersky conta com os pesquisadores mais experientes e respeitados do setor, que contribuem com uma gama de conhecimento e experiência para suas equipes de Segurança da Informação.

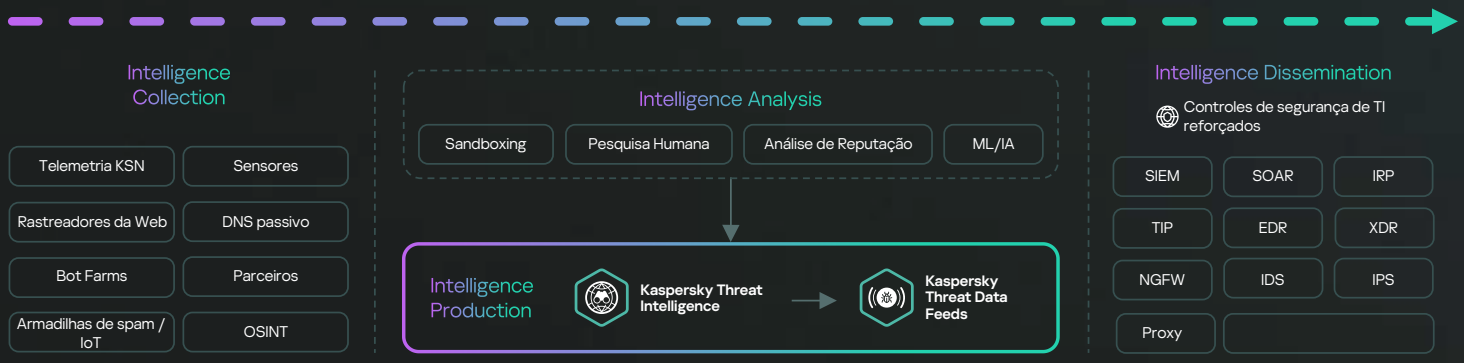
Kaspersky
Threat Data

Feeds do Kaspersky Threat Data

Ciberataques acontecem todos os dias. As ciberameaças estão em constante evolução em termos de frequência, complexidade e ocultação, à medida que tentam comprometer as defesas de suas vítimas. Os criminosos utilizam cadeias de kill chain, campanhas e táticas, técnicas e procedimentos (TTPs) personalizados de intrusão para interromper seus negócios ou causar danos aos seus clientes. Uma proteção eficaz exige novos métodos com inteligência de ameaças como base.

Ao integrar feeds de inteligência de ameaças que são atualizados constantemente - dos quais contém informações 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 categorização de alertas iniciais, fornecendo simultaneamente aos seus especialistas de triagem as informações necessárias para identificar imediatamente alertas que devem ser investigados ou encaminhados para equipes de resposta a incidentes para investigação e resposta adicionais.

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 malwares conhecidos, sites de phishing, vulnerabilidades e exploits mais recentes, além de outros tipos de ciberameaças. Essas informações ajudam você a bloquear tráfego malicioso, manter seus softwares de segurança atualizados e adotar outras medidas para proteger-se contra ciberataques.



1

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.

2

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.

3

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 que?” e identifique a origem dos ataques, permitindo uma tomada de decisão rápida para proteger sua empresa contra ameaças de qualquer complexidade.

Dados contextuais

Os dados contextuais ajudam a mostrar um panorama geral para validação adicional e suporte na utilização dos dados. As entradas de feeds fornecidos pela Kaspersky contêm dados contextuais que ajudam você a confirmar e priorizar ameaças com agilidade:

1. Nomes de ameaças
2. Endereços de IP e nomes de domínio de recursos maliciosos da Web
3. Hashes de arquivos maliciosos
4. Objetos vulneráveis e comprometidos
5. Táticas, técnicas e procedimentos de ataques segundo a classificação MITRE AT&CK
6. Marcação de data e hora
7. Geolocalização
8. Popularidade, e assim por diante...

Benefícios do Kaspersky Threat Data Feeds

Melhore e acelere a resposta a incidentes e os recursos de análise investigativa

ao automatizar o processo de triagem inicial, fornecendo aos seus analistas de segurança contexto suficiente para identificar imediatamente os alertas que precisam ser investigados ou escalados para equipes de resposta a incidentes para qualquer investigação e resposta adicionais.

Reforce suas soluções de segurança

ao incluir SIEMs, firewalls, IPS/IDS, proxy de segurança, soluções de DNS, anti-APT, com indicadores de comprometimento (IOCs) continuamente atualizados, e contexto acionável para fornecer insights sobre ciberataques e uma maior compreensão da intenção, capacidades e dos alvos de seus adversários. Suporte completo para os principais SIEMs (incluindo ArcSight, IBM QRadar, MS Sentinel, Splunk etc.) e plataformas de TI

Detenha ações de exfiltração de materiais confidenciais e propriedade intelectual

de máquinas infectadas para fora da sua organização. Detecte materiais infectados rapidamente para proteger a reputação da sua marca, mantenha sua vantagem competitiva e garanta oportunidades de negócios.

Expanda seus negócios de MSSP

ao fornecer inteligência de ponta contra ameaças como um serviço premium para seus clientes. Como uma CERT, melhore e expanda suas capacidades de detecção e identificação de ciberameaças.

Kaspersky CyberTrace

Kaspersky CyberTrace

O crescimento contínuo no número de feeds de dados de ameaças e fontes de inteligência de ameaças disponíveis torna difícil para as empresas determinar quais informações são realmente relevantes para elas. Ao mesmo tempo, a inteligência de ameaças é fornecida em diversos formatos e inclui muitos indicadores de comprometimento (IoCs), fazendo com que seja difícil para as SIEMs ou outros controles de segurança de rede assimilá-los.

Ao integrar inteligência de ameaças legível por máquina e atualizada em controles de segurança existentes, como sistemas de SIEM, os Centros de Operações de Segurança conseguem automatizar o processo de triagem inicial, fornecendo aos seus analistas de segurança contexto suficiente para identificar imediatamente alertas que precisam ser investigados ou escalados para as equipes de resposta a incidentes para investigação e resposta adicionais.

O Kaspersky CyberTrace é uma plataforma de inteligência contra ameaças que permite a integração perfeita de feeds de dados de ameaças com soluções de SIEM, para ajudar os analistas a aproveitar com mais eficácia a inteligência de ameaças nos fluxos de trabalho das operações de segurança existentes. Ele se integra a qualquer feed de inteligência de ameaças (seja da Kaspersky, de outros fornecedores, OSINT ou seus próprios feeds de clientes) nos formatos JSON, STIX, XML e CSV e oferece suporte à integração imediata com várias soluções de SIEM e fontes de log.

Destaques

Informações detalhadas sobre cada indicador fornecem análises ainda mais profundas. Cada página apresenta todas as informações sobre um indicador de todos os fornecedores de inteligência de ameaças (desduplicação), de modo que os analistas podem discutir ameaças nos comentários e adicionar inteligência de ameaças internas sobre o indicador.

As estatísticas de uso de feeds para medir a eficácia dos feeds integrados e da matriz de interseção de feeds ajudam a escolher os fornecedores de inteligência de ameaças mais valiosos

A marcação de IoCs simplifica o gerenciamento de IoC. Crie qualquer tag, especifique seu peso (importância) e use-a para a marcação manual de IoCs. Você também pode classificar e filtrar IoCs com base nessas tags e seus níveis de importância

O Gráfico de Pesquisa permite a você explorar visualmente os dados e as detecções armazenadas no CyberTrace e descobrir semelhanças entre as ameaças detectadas.

O recurso de exportação de indicadores permite a exportação de conjuntos de indicadores para controles de segurança, como listas de políticas (listas de bloqueios), além do compartilhamento de dados de ameaças entre instâncias do Kaspersky CyberTrace ou com outras plataformas de TI

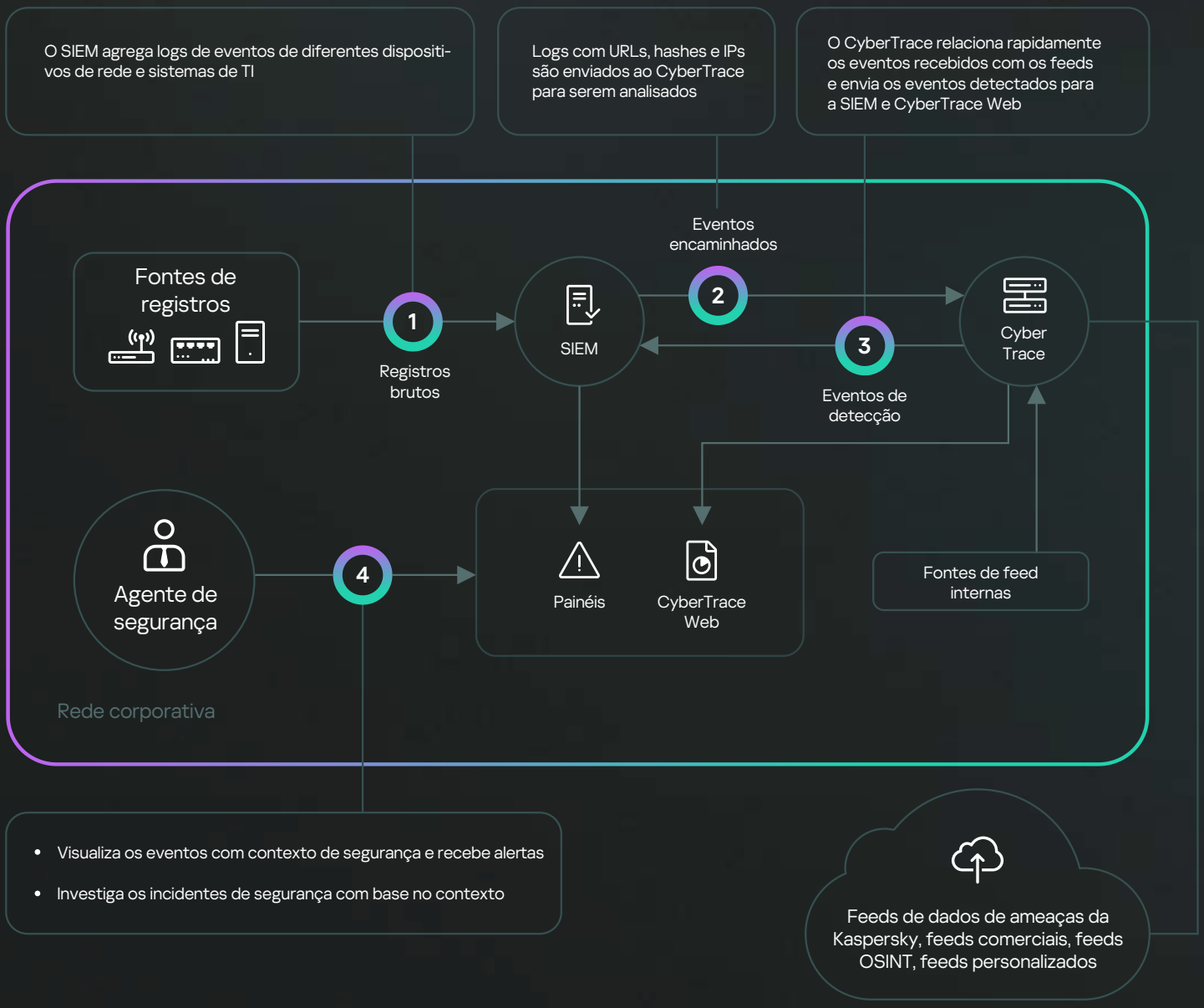
Com o recurso de correlação histórica (retroscan), é possível analisar itens observáveis a partir de eventos verificados anteriormente usando os feeds mais recentes para encontrar ameaças previamente descobertas

O recurso multitenancy (multi-usuários) oferece suporte a MSSPs e casos de uso de grandes empresas

Um filtro envia eventos de detecção para soluções SIEM, reduzindo a carga sobre eles e também sobre os analistas

A HTTP RestAPI permite que você pesquise e gerencie a inteligência de ameaças

Como funciona



O Kaspersky CyberTrace analisa logs e eventos recebidos, combina rapidamente os dados resultantes com os feeds e gera seus próprios alertas de detecção de ameaças.

Benefícios de usar o CyberTrace com os Feeds de Dados de Ameaças da Kaspersky.

Filtrar e priorizar efetivamente grandes quantidades de alertas de segurança

Melhorar e acelerar os processos de triagem e de resposta inicial

Criar uma defesa proativa e orientada por inteligência

Identifique imediatamente alertas críticos para o seu negócio e encaminhe para as equipes de RI

Kaspersky
Threat Lookup

Kaspersky Threat Lookup

O crime virtual não tem fronteiras e as capacidades técnicas estão melhorando rapidamente: os ataques estão cada vez mais sofisticados, pois os criminosos virtuais utilizam recursos da Dark Web para ameaçar seus alvos. As ciberameaças estão em constante crescimento em termos de frequência, complexidade e ocultação, à medida que novas tentativas são realizadas para comprometer as defesas de suas vítimas. Os invasores utilizam kill chains complicadas, e táticas, técnicas e procedimentos (TTP) personalizados nas campanhas para afetar suas operações, roubar seus dados ou causar danos aos seus clientes.

O Kaspersky Threat Lookup oferece todo o conhecimento adquirido pela Kaspersky sobre ciberameaças e como elas funcionam, reunindo tudo em um serviço da Web único e poderoso. O objetivo é fornecer às suas equipes de segurança o maior número de dados possível, prevenindo os ataques virtuais antes que afetem sua organização. A plataforma obtém a inteligência de ameaças detalhada mais recente sobre URL, domínios, endereços de IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS, atributos de arquivos, dados de geolocalização, cadeias de download, carimbos de data/hora, etc. O resultado é a visibilidade global de ameaças novas e emergentes, ajudando você a proteger a sua organização e a melhorar a resposta a incidentes.

Como funciona

Objetos para análise

Destaques

Inteligência Confiável

Um atributo fundamental do Kaspersky Threat Lookup é a confiabilidade dos nossos dados de inteligência de ameaças, enriquecidos com contexto acionável. A Kaspersky é líder no campo dos testes Antimalware, demonstrando a qualidade inigualável da nossa inteligência de segurança ao fornecer as mais altas taxas de detecção, com quase zero falsos positivos

Busca de ameaças

Seja proativo na prevenção, detecção e resposta a ataques, para minimizar seu impacto e frequência. Rastreie e elimine eficientemente os ataques o mais cedo possível. Quanto mais cedo você descobrir uma ameaça, menos danos ela pode causar, mais rápido os reparos ocorrerão e mais cedo as operações de rede poderão voltar ao normal.

Facilidade de uso

Interface Web ou acesso à RESTful API Utilize o serviço no modo manual via uma interface da Web (usando um navegador web) ou acesse-o via uma API RESTful simples — o que você preferir

Uma gama de formatos de exportação

Exporte IOCs (indicadores de comprometimento) ou dados de contexto acionável para formatos de compartilhamento legíveis por máquina mais amplamente utilizados e organizados; como STIX, OpenIOC, JSON, Yara, Snort ou mesmo CSV, para extrair o máximo de benefícios da inteligência contra ameaças, automatizar o fluxo de trabalho das operações ou integrar em controles de segurança como SIEMs.

Análise de Ameaças Kaspersky benefícios

1

Conduza pesquisas profundas sobre indicadores de ameaças em um contexto altamente validado que permite priorizar ataques e focar na mitigação de ameaças que trazem maior risco ao seu negócio

2

Faça diagnósticos e análises de incidentes de segurança em hosts e na rede de maneira mais eficiente, além de priorizar sinais de sistemas internos contra ameaças desconhecidas

3

Aprimore sua resposta a incidentes e funcionalidades de busca de ameaças para desfazer kill chains antes que os sistemas e dados cruciais sejam comprometidos

4

Procurar indicadores de ameaças através de uma interface baseada na Web ou através da API RESTful

5

Examinar detalhes avançados, incluindo certificados, nomes normalmente utilizados, caminhos de arquivo ou URLs relacionadas para descobrir novos objetos suspeitos

6

Verifique se o objeto descoberto pode ser considerado uma ameaça já disseminada ou única, e entenda por que um objeto deve ser tratado como malicioso

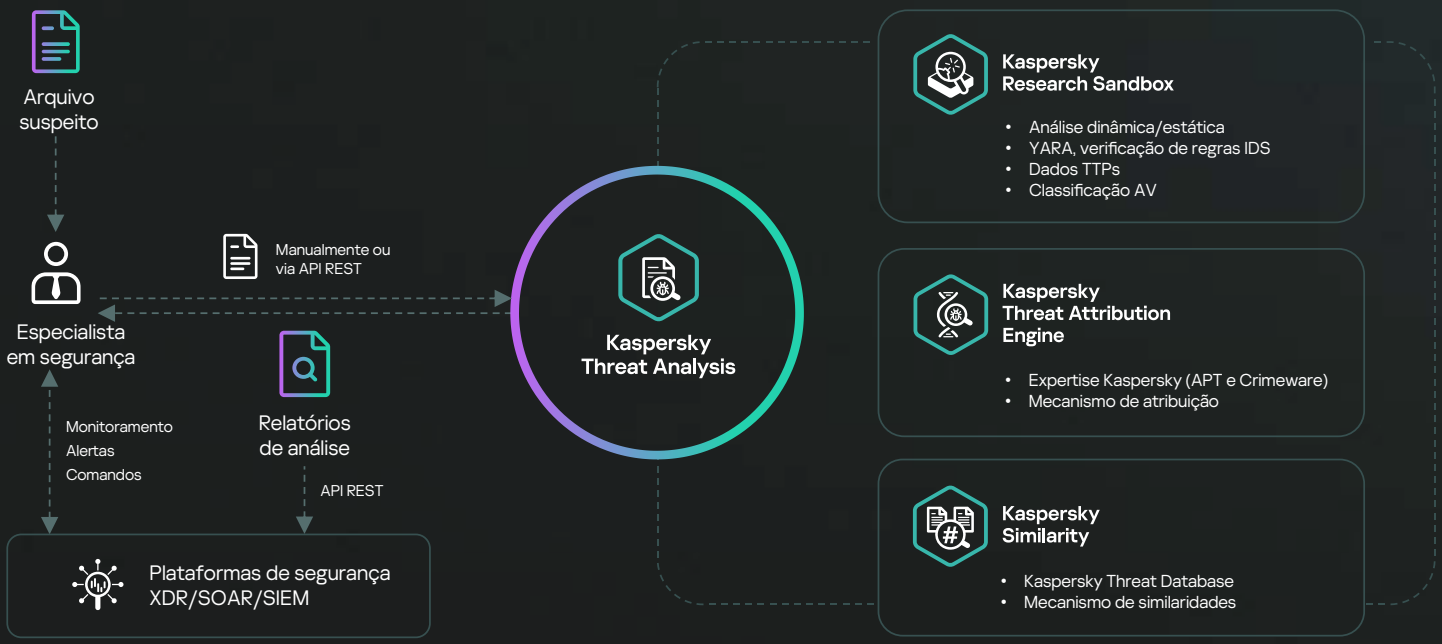
Kaspersky
Threat Analysis

Kaspersky Threat Analysis

Diante de uma ciberameaça em potencial, suas decisões e sua capacidade de ação podem ser ambos cruciais. É impossível prever todos os ataques direcionados da atualidade usando apenas ferramentas de antivírus tradicionais. Mecanismos antivírus conseguem deter apenas as ameaças conhecidas e suas variantes, enquanto agentes de ameaças sofisticados utilizam todos os meios à sua disposição para escapar da detecção automática. A quantidade de alertas de segurança processados pelos SOCs diariamente cresce exponencialmente. Com o volume de amostras de malware geradas diariamente, a priorização de alertas eficazes, triagem e validação se torna ainda mais inviável.

Para ajudar os investigadores de segurança a se manterem informados sobre ameaças emergentes, a Kaspersky fornece uma estrutura única resiliente para automatizar a análise de rotina de arquivos suspeitos. Além da tecnologia de análise de ameaças tradicional como sandbox, o Kaspersky Threat Analysis fornece a você tecnologias de similaridade relacionadas e capacidade de atribuição de ponta. Essa é uma abordagem híbrida que proporciona uma análise de ameaças eficiente, para que você possa tomar decisões, dispondo de todas as informações para manter sua infraestrutura em segurança. A Análise de Ameaças da Kaspersky é fornecida por meio de interfaces web unificadas e RESTful.

Análise de Ameaças Kaspersky componentes



Kaspersky
Research Sandbox

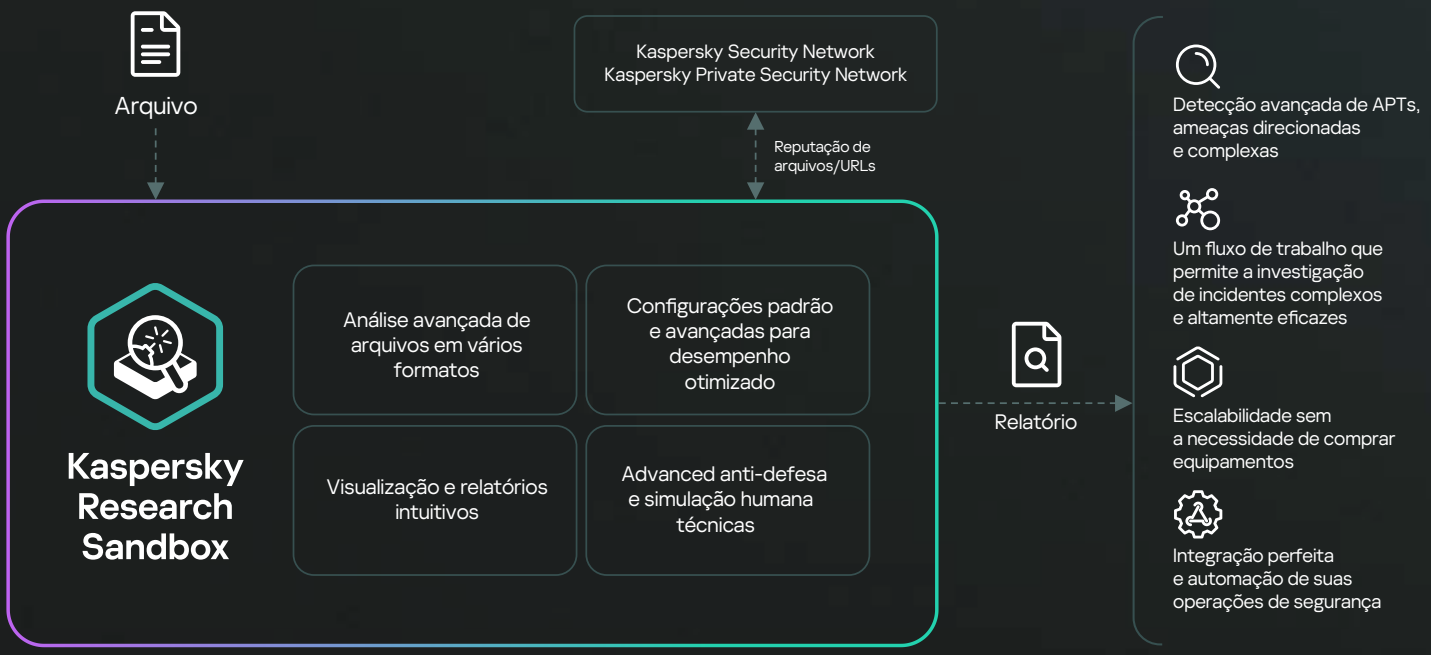
Kaspersky Research Sandbox

O Kaspersky Research Sandbox foi desenvolvido diretamente em nosso complexo de sandboxing em laboratório, uma tecnologia que está evoluindo há décadas. A solução incorpora todo o conhecimento sobre comportamentos de malware, adquiridos graças à nossa constante pesquisa sobre ameaças, possibilitando a detecção de mais de 420 mil novos objetos maliciosos diariamente.

O Kaspersky Research Sandbox permite investigar as origens de amostras de arquivos, coletar IOCs com base em análise comportamental e detectar objetos maliciosos que passaram despercebidos anteriormente. Ele oferece uma abordagem híbrida, combinando análise comportamental e técnicas anti-evasão sólidas, com tecnologias que simulam o comportamento humano, como auto clicker, rolagem de documentos e processos fictícios.

Implementada localmente, essa nova tecnologia avançada também evita a exposição de dados fora do perímetro da organização. O Kaspersky Research Sandbox on-premise também permite criar ambientes de execução personalizados, adaptado para ambientes reais, o que aumenta a precisão da detecção de ameaças e a velocidade de investigação.

Como funciona



Destaques de produtos

- Tecnologia patenteada
- Análise de objetos automatizada em ambientes Windows, Linux e Android
- Suporte à análise de mais de 200 tipos de arquivos com relatórios de análise detalhados
- +1000 caças únicas para extração de TTPs pela MITRE ATT&CK
- Técnicas anti-evasão avançadas e tecnologias de simulação humana
- A pontuação de ameaças com base em métricas e dados obtidos durante a execução de arquivos mostra o nível de perigo do objeto analisado
- Regras pré-configuradas do Suricata para inspecionar o tráfego de rede gerado durante a execução de arquivos.
- Upload manual de amostras e API REST aprimorada para integração com fluxos de trabalho automatizados

Kaspersky
Threat Attribution
Engine

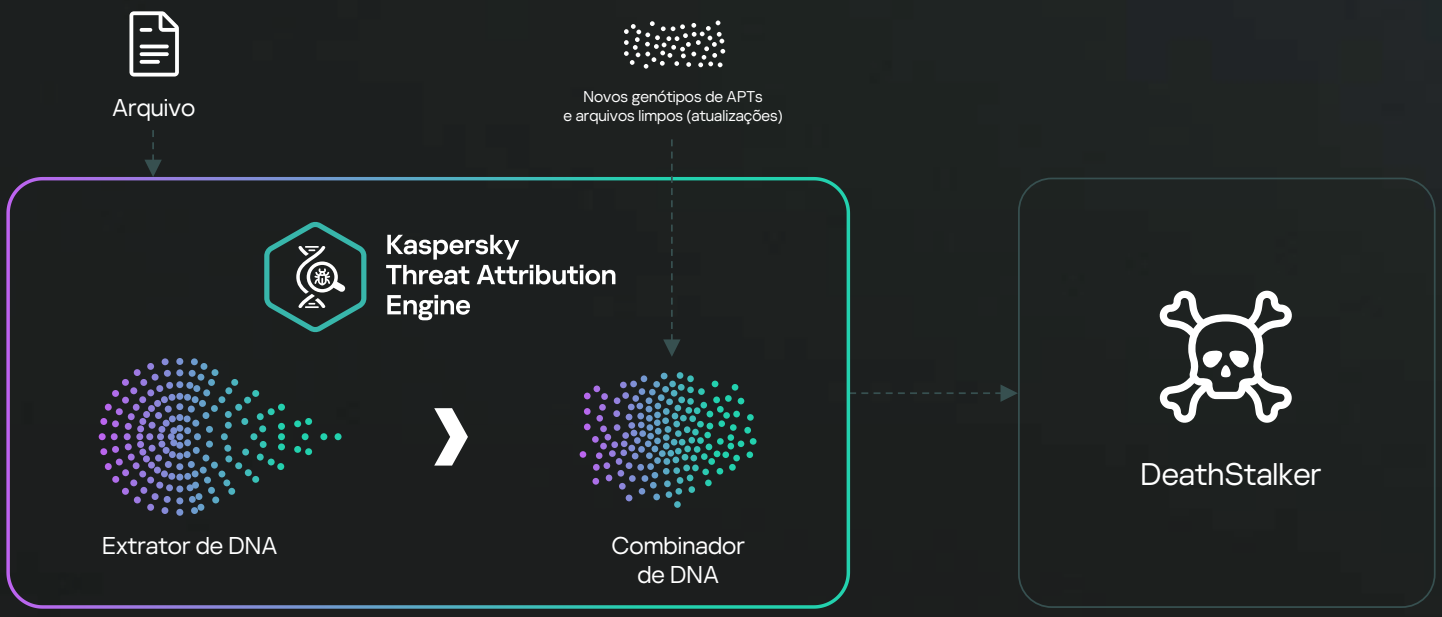
Kaspersky Threat Attribution Engine

O Kaspersky Threat Attribution Engine é uma ferramenta única de análise de ameaças, que fornece insights sobre a origem de malwares de alto nível e seus possíveis agentes. A solução conecta rapidamente um arquivo suspeito a ameaças APT, agentes e campanhas conhecidos, usando um algoritmo exclusivo e bancos de dados especiais compreendendo amostras de malware APT e a coleta mais ampla do mercado para arquivos limpos, extraídos por especialistas Kaspersky durante mais de 25 anos.

Rastreamos mais de 1.100 agentes e campanhas de ameaças e lançamos mais de 200 relatórios de inteligência de ameaças por ano. A pesquisa contínua apoia a coleta de APTs, contendo mais de 80 mil arquivos que, em conjunto com o uso de ferramentas automatizadas, resulta em níveis altamente precisos de atribuição.

O produto oferece uma abordagem exclusiva para comparar amostras semelhantes, garantindo taxas de falsos positivos quase nulas. Qualquer ataque novo pode ser rapidamente vinculado a um malware de APT, a ataques direcionados anteriores e grupos de hackers, o que ajuda a identificar a ameaça de maior risco dentre incidentes menos importantes, além de permitir a tomada de medidas protetivas em tempo hábil para evitar que um invasor tenha acesso ao sistema. O produto Kaspersky Threat Attribution Engine pode ser implementado em um ambiente seguro de modo a restringir o acesso de terceiros às informações processadas e objetos enviados. A implantação no local fornece funcionalidades adicionais para adicionar atores e amostras próprias para detectar amostras semelhantes a arquivos em sua coleção privada, bem como exportar regras YARA para uma busca automatizada adicional de arquivos semelhantes em sua infraestrutura e integração com soluções de terceiros.

Como funciona



Método de pesquisa proprietário

Para vincular um malware a entidades de atribuição, o Kaspersky Threat Attribution Engine usa um método próprio exclusivo para procurar semelhanças entre arquivos.
da busca por genótipos e sequências semelhantes entre arquivos. O método envolve:

1

Analisar a genética de uma amostra extraindo os seguintes elementos de seu código:

- Genótipos — blocos distintos de código binário.
- Strings — strings distintas de caracteres.

2

Pesquisa automática nos arquivos analisados de genótipos e strings semelhantes a genótipos e strings de amostras APT previamente analisadas ou já vinculadas a entidades de atribuição.

3

Com base em genótipos e sequências semelhantes encontrados em amostras APT, fornecendo um relatório sobre a origem da amostra analisada, entidades de atribuição relacionadas e quaisquer semelhanças entre esta amostra e amostras APT conhecidas.

Destaques do produto

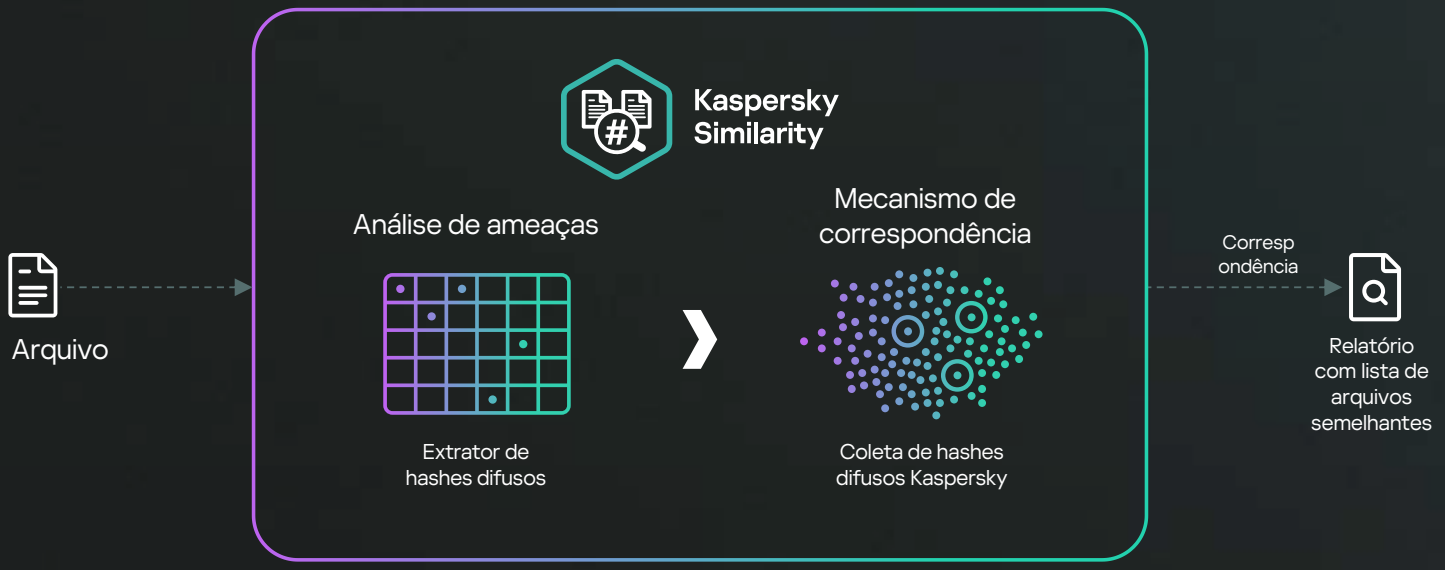
- Tecnologia patenteada
- Fornece acesso imediato a um repositório de dados selecionados sobre centenas de agentes e amostras de APT.
- Upload manual de amostras e API REST aprimorada para integração com fluxos de trabalho automatizados
- Funcionalidade para descompactar arquivos protegidos por senha com senhas personalizadas
- Exportação para o formato STIX 2.1 (os formatos TXT e JSON também são suportados) para análise automatizada adicional de logs de segurança ou integração com soluções/controles de segurança terceirizados
- Oferece suporte à implantação no Amazon Web Services (AWS), permitindo configuração rápida do produto e economia de custos, pois não há necessidade de investir antecipadamente em hardware

Kaspersky Intelligence Reporting

Análise de similaridades Kaspersky

O Kaspersky Similarity é uma ferramenta útil para identificar arquivos com funcionalidades semelhantes, com base na tecnologia desenvolvida por especialistas da Kaspersky para proteção contra ameaças desconhecidas e ocultas. A tecnologia utiliza mais de 50 tipos únicos de hashes especiais e um banco de dados de amostras de malware acumuladas pela Kaspersky ao longo de 25 anos e contendo milhões de arquivos maliciosos para garantir a maior precisão e confiabilidade dos resultados.

Encontre malware semelhantes (evasivos) e busque pela infraestrutura, para ter certeza que qualquer ligeira modificação na amostra feita pelos criminosos não escapará do seu radar.



Relatórios de similaridade

Os especialistas Kaspersy criaram um conjunto de hashes para determinar a similaridade entre diferentes arquivos, com base nesses atributos.

O Kaspersky Similarity permite aos usuários enviar um arquivo suspeito, extrair os hashes difusos e compará-los àqueles de arquivos do banco de dados de ameaças da Kaspersky. No caso de uma correspondência ser identificada, a solução gera uma lista de hashes para os principais arquivos maliciosos semelhantes e já conhecidos da Kaspersky, classificados por uma pontuação de similaridade. O relatório contém contexto adicional, com metadados para cada arquivo similar encontrado:

- Grau de confiança de similaridade
- Status do arquivo (malware, adware ou outro)
- Nome da ameaça
- Carimbos de hora da primeira e última detecção
- Quantidade de ocorrências (detecções)
- Hash de arquivos
- Tipo de arquivo
- Tamanho do arquivo

Destaques

- Tecnologia patenteada
- A solução tira proveito do maior banco de dados de arquivos limpos e maliciosos do mercado, coletados ao longo de mais de 25 anos de experiência, permitindo a mais ampla cobertura para uma alta precisão de comparação
- Upload manual de amostras e API REST aprimorada para integração com fluxos de trabalho automatizados
- A solução já é amplamente usada pelos especialistas Kaspersky para explorar novas ameaças e fornecer uma alta proteção nos nossos produtos, regularmente comprovada pelas altas taxas de avaliação positivas em testes independentes:

Saiba mais

Análise de Ameaças Kaspersky benefícios

1

Aprimore suas atividades de resposta a incidentes e forense com o Kaspersky Research Sandbox, que oferece uma análise dinâmica de ponta de arquivos suspeitos com a capacidade de encontrar ameaças 0-day e resultados mapeados para as TTPs do MITTRE ATT&ACK.

2

A atribuição correta e oportuna com o Kaspersky Threat Attribution Engine ajuda a definir o ator de ameaças com a lista completa de TTPs, proporcionando uma visão abrangente do vetor de ataque com etapas claras de mitigação, permitindo encurtar o tempo de resposta a incidentes de meses para minutos.

3

Revele ameaças evasivas com o Kaspersky Similarity, que permite encontrar amostras maliciosas que foram especialmente criadas para contornar as tecnologias antimalware tradicionais, a fim de detectar os ataques APT mais sofisticados que podem durar anos sem serem rastreados.

Kaspersky Intelligence Reporting

Relatórios de Inteligência contra Ameaças da Kaspersky

A neutralização de ameaças virtuais modernas requer uma visão de 360° das táticas e ferramentas utilizadas por seus agentes. Embora os C&Cs e as ferramentas usadas em ataques mudem com frequência, é difícil para os atacantes mudarem seu comportamento e métodos durante a execução do ataque. Identificar e expor esses padrões prontamente ajuda a implantar mecanismos defensivos eficazes antecipadamente, desarmar os cibercriminosos e interromper a cadeia de ataque.

A assinatura do Kaspersky Threat Intelligence Reporting fornece acesso exclusivo contínuo à nossa pesquisa, oferecendo informações atualizadas sobre as ameaças mais perigosas, permitindo que você e sua equipe de segurança apliquem proativamente uma estratégia eficaz para detecção de ataques de forma oportuna, além de minimizar os danos de ameaças semelhantes.

Embora apenas uma pequena porcentagem de nossas investigações seja tornada pública, o Kaspersky Intelligence Reporting oferece acesso privilegiado às informações mais atualizadas sobre as últimas ameaças. Nossos especialistas monitoram continuamente as atividades de cibercriminosos, identificando os ataques direcionados mais sofisticados e perigosos, campanhas de espionagem cibernética, amostras de malware e criptografia, e as últimas tendências em cibercrime ao redor do mundo.

Mais de 200
relatórios privados por ano

Mais de 300
agentes de ameaças

Mais de 500
virtual

Mais de 2500
Regras YARA

170.000+
IoCs

Os relatórios analíticos incluem:

Perfis de agentes de ameaça

Mapeamento para MITRE ATT&CK

Resumo executivo (Informações orientadas para C-level)

A análise técnica profunda inclui:

- Métodos de ataque
- Exploits usados
- Descrição de malware
- Infraestrutura C&C e descrição de protocolos
- Análise da vítima
- Análise de exfiltração de dados
- Atribuições

Indicadores de compromisso (IOCs) e regras YARA / SIGMA / Suricata

Recomendações dos especialistas da Kaspersky

Oferecemos várias opções de trilhas de relatórios comerciais com base em suas necessidades e nas especificidades de sua organização:

Kaspersky APT Intelligence Reporting

Fornece insights sobre ameaças cibernéticas sofisticadas e direcionadas a longo prazo, que frequentemente têm origem em grupos bem organizados e bem financiados. Inclui informações sobre vários grupos APT em todo o mundo e suas táticas, técnicas e procedimentos (TTPs), bem como os setores e regiões que eles visam. Esta linha de relatório concentra-se em atividades de espionagem, abrangendo desde ataques à cadeia de suprimentos até atividades hacktivistas e destrutivas. Esses relatórios são ideais se a sua organização for uma grande corporação, agência governamental ou uma organização envolvida em infraestrutura crítica, e também são particularmente relevantes para organizações que possuem dados confidenciais que podem ser objeto de interesse de entidades governamentais.

Kaspersky Crimeware Intelligence Reporting

Concentra-se em ataques e campanhas tendo como objetivo principal o ganho financeiro. Inclui informações sobre as últimas tendências em crimes cibernéticos, incluindo dados roubados vendidos na darkweb, fraude financeira, ransomware e malware ATM/PoS. Eles fornecem detalhes sobre novas variedades de crimeware, seus métodos de distribuição e os tipos de dados que visam. Este acompanhamento de relatórios é particularmente relevante se a sua organização conduz uma quantidade substancial de negócios on-line ou se você mantém dados confidenciais de clientes - talvez como uma instituição financeira ou plataforma de comércio eletrônico.

Kaspersky ICS Threat Intelligence

O ICS Threat Intelligence Reporting fornece inteligência aprofundada e maior conscientização sobre campanhas maliciosas que visam organizações industriais, bem como informações sobre vulnerabilidades encontradas nos mais populares sistemas de controle industrial e tecnologias subjacentes. Este acompanhamento de relatórios é fornecido pelo Kaspersky ICS CERT – uma equipe dedicada de mais de 30 especialistas altamente qualificados em pesquisa de ameaças e vulnerabilidades de ICS, resposta a incidentes e análise de segurança, criada em 2016. Fornecidos pelo ICS CERT da Kaspersky, esses relatórios fornecem insights e orientações acionáveis para proteger propriedades digitais e físicas críticas, incluindo componentes de software e hardware, garantindo a segurança e a continuidade dos processos tecnológicos.

Você pode considerar os seguintes serviços relacionados ao Kaspersky ICS Threat Intelligence:

ICS Threat Intelligence Reporting

Assinatura de nossas publicações regulares sobre ameaças e vulnerabilidades à segurança cibernética industrial:

- Alertas sobre ameaças dia 0
- Relatórios técnicos detalhados
- Avaliações mensais
- Recomendações sobre mitigação de vulnerabilidades
- Notícias e tendências

Feeds de dados de ameaças ICS

Fluxos de dados legíveis por máquina sobre ameaças e vulnerabilidades de cibersegurança industrial.

Formatos simples de distribuição de dados (JSON, CSV, OpenIoC, STIX) via HTTPS, TAXII e métodos de entrega especializados para integração em soluções de segurança da informação.

Ask the Analyst

Consulta com especialistas da Kaspersky ICS CERT, fornecendo a você conselhos individuais sobre ameaças e vulnerabilidades de cibersegurança industrial, estatísticas e panorama de ameaças, padrões da indústria, etc, mais relevantes para você.

Relatório de Inteligência de Ameaças da Kaspersky Threat Intelligence fornece a você:

Acesso privilegiado

Por várias razões, nem todas as ameaças de alto nível são divulgadas ao público em geral. No entanto, fornecemos esse tipo de informação exclusiva para nossos clientes durante o processo de investigação, mesmo antes do anúncio público oficial.

Acesso a dados técnicos

Inclui uma lista ampla de IOCs disponíveis nos formatos padrão, que incluem o openIOC ou o STIX, bem como acesso às nossas regras YARA / Sigma / Suricata

Perfis de agentes de ameaça

Incluindo o país de origem suspeito e a atividade principal, famílias de malware usadas, setores e regiões visadas e descrições de todos os TTPs usados, com mapeamento para MITRE ATT&CK

MITRE ATT&CK

Todos os TTPs descritos nos relatórios são mapeados para o MITRE ATT&CK, permitindo uma melhor detecção e resposta através do desenvolvimento e priorização dos casos de uso de monitoramento de segurança correspondentes, efetuando análises de falhas e testando as defesas atuais contra aos TTPs relevantes.

Análise retrospectiva

É fornecido acesso a todos os relatórios privados disponíveis durante todo o período da assinatura.

Suporte API RESTful

Integração e automação perfeitas dos seus fluxos de trabalho de segurança

Kaspersky
Digital Footprint
Intelligence

Kaspersky Digital Footprint Intelligence

À medida que a sua empresa expande, a complexidade e a distribuição dos seus ambientes de TI também cresce, criando um desafio: proteger sua presença digital distribuída sem controle direto ou propriedade. Ambientes dinâmicos e interconectados permitem que as empresas obtenham benefícios significativos. No entanto, a interconetividade em constante crescimento está também expandindo a superfície de ataque. À medida que os invasores adquirem mais competências, é vital ter uma visão exata da presença online da sua organização, mas também monitorar suas mudanças e reagir a informações atualizadas sobre materiais digitais expostos.

As organizações usam uma ampla gama de ferramentas de segurança em suas operações de segurança, mas ainda existem ameaças digitais que exigem recursos muito específicos - para detectar e mitigar vazamentos de dados, monitorar planos e esquemas de ataque de cibercriminosos localizados em fóruns da dark web, etc. Para ajudar os analistas de segurança a explorar a visão do adversário sobre os recursos da sua empresa, ou descobrir a tempo os potenciais vetores de ataque em sua organização e ajustar as defesas de acordo, a Kaspersky criou o Kaspersky Digital Footprint Intelligence.

O Kaspersky Digital Footprint Intelligence fornece

Detecção de ameaças

Monitoramento de atividades fraudulentas que podem prejudicar a reputação de uma empresa e/ou decepcionar os clientes.

Reconhecimento de rede

Identificação dos recursos de rede do cliente e serviços expostos que são um potencial ponto de entrada para um ataque. Análise personalizada das vulnerabilidades existentes, com pontuação e avaliação de risco abrangente adicionais baseadas na pontuação base do CVSS, disponibilidade de exploits públicos, experiência de testes de penetração e localização do recurso da rede (hospedagem/infraestrutura).

Monitoramento da Dark Web

Monitoramento contínuo de domínios e recursos da Dark Web (fóruns, blogs de ransomware, messengers, sites portais etc.) para detectar quaisquer referências e ameaças relacionadas à sua empresa, clientes e parceiros. Análise de ataques direcionados ativos ou ataques que estejam sendo planejados, campanhas de APT direcionadas à sua empresa, setor ou região de operações.

Detecção de vazamentos de dados

Detecção de dados comprometidos de colaboradores, credenciais de parceiros e clientes, cartões bancários, números de telefone e outras informações confidenciais que podem ser usadas para perpetrar um ataque ou podem representar riscos para a reputação da empresa.

Suporte para multilocação

Recursos incrementados para provedores de serviços de segurança gerenciada (MSSPs) e organizações de grande porte com estrutura de filiais.

Fontes de inteligência

É vital que você adquira uma compreensão abrangente do seu nível de segurança externa.
Para fornecer essas informações, os analistas de segurança Kaspersky coletam e agregam informações extraídas das seguintes fontes de inteligência:

Seus dados não estruturados

- Endereços de IP
- Domínios da empresa
- Nomes de marcas
- Palavras-chave
- Alcances de rede
- Números de cartão BIN/IIN
- Informações de funcionários

Inventário de perímetro de rede

Busca na web superficial, profunda e obscura

Busca na base de Conhecimento da Kaspersky

Alertas de ameaças

Pesquisa em tempo real pelos recursos da Kaspersky, Internet e Dark Web

Relatórios analíticos*

Como funciona

Configuração

Descoberta de informações sobre ativos digitais da empresa

Coleta

Coleta automatizada de dados da internet, deep e dark webs e da base de conhecimento Kaspersky

Filtro

Detecção, análise e priorização de ameaças gerenciadas por analistas

Notificação

Fornecimento de notificações sobre ameaças operacionais no Portal Kaspersky Threat Intelligence via API

*Serviço complementar

Inteligência de Pegada Digital valores comerciais

O Kaspersky Digital Footprint Intelligence oferece benefícios e alto valor agregado para a sua organização:

Detecção de ameaças

Detecte ameaças potenciais em tempo real e proteja a reputação da sua empresa, preservando a confiança dos clientes, reduzindo o risco de prejuízos financeiros e danos às operações comerciais.

Reduza os riscos cibernéticos

Equipe seus principais agentes (diretoria e gestão) com informações sobre onde concentrar os gastos com cibersegurança, expondo deficiências na configuração atual e os riscos que elas representam.

Reaja com agilidade

O contexto adicional para alertas de segurança aprimora a resposta a incidentes e reduz o tempo médio de resposta (MTTR)

Reduza sua superfície de ataque

Gerencie a presença digital da sua empresa e controle os recursos de rede externos para combater vetores de ataque e vulnerabilidades que podem ser usados em um ataque.

Entre na mente de seus adversários

Prevenção e antecipação - saiba o que os cibercriminosos estão planejando e o que estão falando sobre a sua empresa na dark web e para que você possa estar preparado em caso de um ataque.

Domine o desconhecido

Melhore sua capacidade de resistir a ciberataques e de identificar ameaças fora do perímetro das equipes de segurança interna.

Eficiência na entrega de serviços

O início rápido e a escalabilidade fácil no modo de multilocação economizam tempo tanto para os provedores de serviços de segurança gerenciados (MSSP) quanto para seus clientes, bem como para grandes organizações multi-afiliadas.

Kaspersky Takedown Service

Kaspersky Takedown Service

Os cibercriminosos criam domínios maliciosos e de phishing que são usados para atacar sua empresa e suas marcas. A incapacidade de eliminar rapidamente essas ameaças, após serem identificadas, pode levar à perda de receita, danos à marca, perda de confiança dos clientes, vazamentos de dados e muito mais. Mas gerenciar o derrubamento desses domínios é um processo complexo, que requer experiência e tempo.

O Kaspersky Takedown Servicecombate rapidamente as ameaças de domínios maliciosos e de phishing antes que qualquer dano possa ser causado à sua marca e aos seus negócios. O gerenciamento de ponta a ponta de todo o processo economiza tempo e recursos valiosos dos clientes. O serviço de Takedown é fornecido globalmente.

A Kaspersky bloqueia mais de 15 mil URLs de phishing/scam e impede mais de um milhão de tentativas de clicar nesses URLs todos os dias. Graças aos vários anos de experiência na análise de domínios maliciosos e de phishing, sabemos como coletar todas as evidências necessárias para provar que eles são maliciosos. Cuidaremos do seu gerenciamento de remoção e permitiremos uma ação rápida para minimizar seu risco digital para que sua equipe possa se concentrar em outras tarefas prioritárias.

A Kaspersky oferece aos seus clientes proteção eficaz dos seus serviços online e reputação, trabalhando com organizações internacionais, agências nacionais e regionais de polícia (por exemplo, INTERPOL, Europol, Unidade de Crimes Digitais da Microsoft, Unidade Nacional de Crimes de Alta Tecnologia (NHTCU) da Agência Policial dos Países Baixos e The City of London Police), bem como Computer Emergency Response Teams (CERTs) em todo o mundo.

Visibilidade completa

Você receberá notificações a cada etapa do processo, desde o registro da sua solicitação até a derrubada bem-sucedida

Gerenciamento de ponta a ponta

Gerenciaremos todo o processo de remoção e minimizaremos seu envolvimento.

Cobertura global

Seja qual for o local em que um domínio malicioso ou de phishing está registrado, a Kaspersky solicitará sua remoção da organização regional com a autoridade legal relevante.

Como funciona?

Você pode solicitar diretamente através da Conta Corporativa Kaspersky, no nosso portal de suporte ao cliente corporativo. Prepararemos toda a documentação necessária e enviaremos a solicitação de remoção à autoridade local/regional relevante (CERT, registrador, etc.) que tenha os direitos legais necessários para encerrar o domínio. Você receberá notificações em todas as etapas até que o domínio solicitado seja derrubado com sucesso.

Proteção fácil de gerenciar

O Kaspersky Takedown Service elimina rapidamente as ameaças representadas por domínios maliciosos e de phishing antes que qualquer dano possa ser causado à sua marca e aos seus negócios. O gerenciamento de ponta a ponta de todo o processo economiza tempo e recursos valiosos.

Kaspersky
Ask the Analyst

Kaspersky Ask the Analyst

Cibercriminosos estão constantemente desenvolvendo novas formas sofisticadas de atacar empresas. O cenário de ameaças instável e de rápido crescimento da atualidade demonstra o uso de técnicas de ciberataques cada vez mais ágeis. As organizações enfrentam incidentes complexos causados por ataques em formato non-malware, fileless, do tipo living-off-the-land, exploits de dia zero, além de combinações de todas essas variantes incorporadas em ameaças complexas, ataques semelhantes a APT e direcionados.

Em uma época dominada por ciberataques direcionados a empresas de todos os tamanhos, profissionais de cibersegurança são mais importantes do que nunca, mas encontrá-los e retê-los não é tarefa fácil. E mesmo com uma equipe de cibersegurança bem estabelecida, seus especialistas nem sempre estão prontos para lutar na guerra contra ameaças sofisticadas sozinhos— eles precisam ser capazes de recorrer à assistência especializada de terceiros. A experiência externa pode esclarecer os caminhos prováveis de ataques complexos e APTs, fornecendo conselhos acionáveis sobre as melhores maneiras de eliminá-los.

A pesquisa de ameaças constante permite que a Kaspersky descubra, se infiltre e monitore comunidades fechadas e fóruns clandestinos frequentados por cibercriminosos em todo o mundo. Nossos analistas aproveitam o acesso à esses fóruns ocultos para detectar e investigar proativamente as ameaças mais prejudiciais e populares, bem como ameaças projetadas para organizações específicas

O serviço Kaspersky Ask the Analyst amplia mais ainda nosso Portfólio de Inteligência de Ameaças, permitindo que você solicite orientação e informações sobre ameaças específicas que está enfrentando ou nas quais está interessado. O serviço adapta os poderosos recursos de inteligência e pesquisa de ameaças da Kaspersky às suas necessidades específicas, permitindo que você monte defesas resilientes contra ameaças direcionadas à sua organização.

Kaspersky Ask the Analyst Deliverables(assinatura unificada mediante solicitação)

APT e Crimeware

Informações adicionais sobre relatórios publicados e pesquisas em andamento (além do serviço APT ou Crimeware Intelligence Reporting)

Descrições de ameaças, vulnerabilidades e IoCs relacionados

- Descrição geral de famílias específicas de malware
- Contexto adicional para ameaças (hashes relacionados, URLs, CNCs etc.)
- Informações sobre uma vulnerabilidade específica (nível de gravidade e os mecanismos de proteção correspondentes nos produtos Kaspersky)

Solicitações relacionadas a ICS

- Informações adicionais sobre relatórios publicados
- Informações sobre vulnerabilidade do ICS
- Estatísticas e tendências de ameaças do ICS para região/setor
- Informações de análises de malware do ICS sobre regulamentações ou padrões

Inteligência de Dark Web

- Pesquisa na Dark Web sobre artefatos específicos, endereços de IP, nomes de domínio, nomes de arquivos, e-mails, links ou imagens
- Pesquisa e análise de informações

Malware analysis

- Análise de amostras de malware
- Recomendações sobre novas ações de remediação

Como funciona

O Kaspersky Ask the Analyst pode ser comprado separadamente ou adicionado a qualquer um de nossos serviços de inteligência contra ameaças. Você pode solicitar diretamente através da Conta Corporativa Kaspersky, no nosso portal de suporte ao cliente corporativo. Responderemos por e-mail, mas se caso necessário e você estiver de acordo, podemos agendar uma teleconferência e/ou sessão com compartilhamento de tela para esclarecimentos. Após aceitar a sua solicitação, você receberá informações sobre o tempo estimado de processamento.

Casos de uso

1. Esclareça todos os detalhes em relatórios de inteligência de ameaças publicados anteriormente
2. Obtenha inteligência adicional para IoCs já fornecidos
3. Obtenha detalhes sobre vulnerabilidades e recomendações sobre como proteger-se contra exploits
4. Receba detalhes adicionais sobre as atividades específicas da Dark Web nas quais você está interessado
5. Obtenha um relatório geral da família de malware, incluindo o comportamento do malware, seu impacto potencial e detalhes sobre qualquer atividade relacionada que a Kaspersky tenha observado
6. Priorize efetivamente alertas/incidentes com informações contextuais detalhadas, além de categorização para IoCs relacionados fornecidas por meio de relatórios sintéticos
7. Solicite assistência para identificar se a atividade incomum detectada está relacionada a um APT ou agente de Crimeware
8. Envie arquivos de malware para análises completas, ajudando você a compreender o comportamento e a funcionalidade das amostras fornecidas

Benefícios do Kaspersky Ask the Analyst

Amplie seu conhecimento

Tenha acesso sob demanda a especialistas do setor, sem a necessidade de procurar ou investir na contratação de profissionais que são muitas vezes difíceis de encontrar

Acelere o processo de investigação

Classifique e priorize incidentes eficazmente com base em informações contextuais detalhadas e personalizadas

Reaja rapidamente

Responda a ameaças e vulnerabilidades rapidamente, graças às nossas orientações sobre como bloquear ataques causados por vetores já conhecidos

Amplie seu conhecimento e recursos

O Kaspersky Ask the Analyst, oferece acesso à equipe principal de pesquisadores da Kaspersky, em uma base individualizada. O serviço oferece uma comunicação abrangente entre os especialistas para expandir suas capacidades atuais com nosso conhecimento e recursos exclusivos.

Conclusão

Combater as ciberameaças atuais requer uma visão a 360 graus das táticas e ferramentas utilizadas pelos agentes das ameaças. Gerar essa inteligência e a identificar as contramedidas mais eficazes requer dedicação constante e altos níveis de especialização. Com petabytes de dados complexos de ameaças para extrair, tecnologias avançadas de Machine Learning e um grupo exclusivo de especialistas mundiais, nós trabalhamos para oferecer suporte aos nossos clientes do mundo todo com a mais recente inteligência de ameaças, ajudando-os a manter sua imunidade até mesmo em caso de ciberataques nunca vistos anteriormente.

Principais benefícios

Permite a visibilidade global de ameaças, a detecção imediata de ameaças virtuais, a priorização de alertas de segurança e uma resposta eficaz a incidentes de segurança da informação

Os insights exclusivos sobre as táticas, técnicas e procedimentos usados por agentes de ameaças em diferentes setores e regiões, permitem proteção proativa contra ameaças direcionadas e complexas

Uma visão geral abrangente da sua postura de segurança com recomendações acionáveis sobre estratégias de mitigação permite que você concentre sua estratégia defensiva em áreas identificadas como principais alvos de ataques virtuais

Poupa seus analistas e ajuda a focar sua força de trabalho em ameaças reais

Recursos aprimorados e acelerados de resposta a incidentes e busca de ameaças ajudam a reduzir o "tempo de permanência" do ataque e minimizar significativamente possíveis danos

Kaspersky Threat Intelligence

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture