Kaspersky Threat Intelligence

kaspersky PREPARADOS PARA O FUTURO

Desafio

Monitorar, analisar, interpretar e mitigar as ameaças de segurança de TI em constante evolução é uma tarefa assombrosa. Empresas de todos os setores estão a passar por uma escassez de dados relevantes atualizados, necessários para ajudar a gerir os riscos associados às ameaças de segurança de TI.

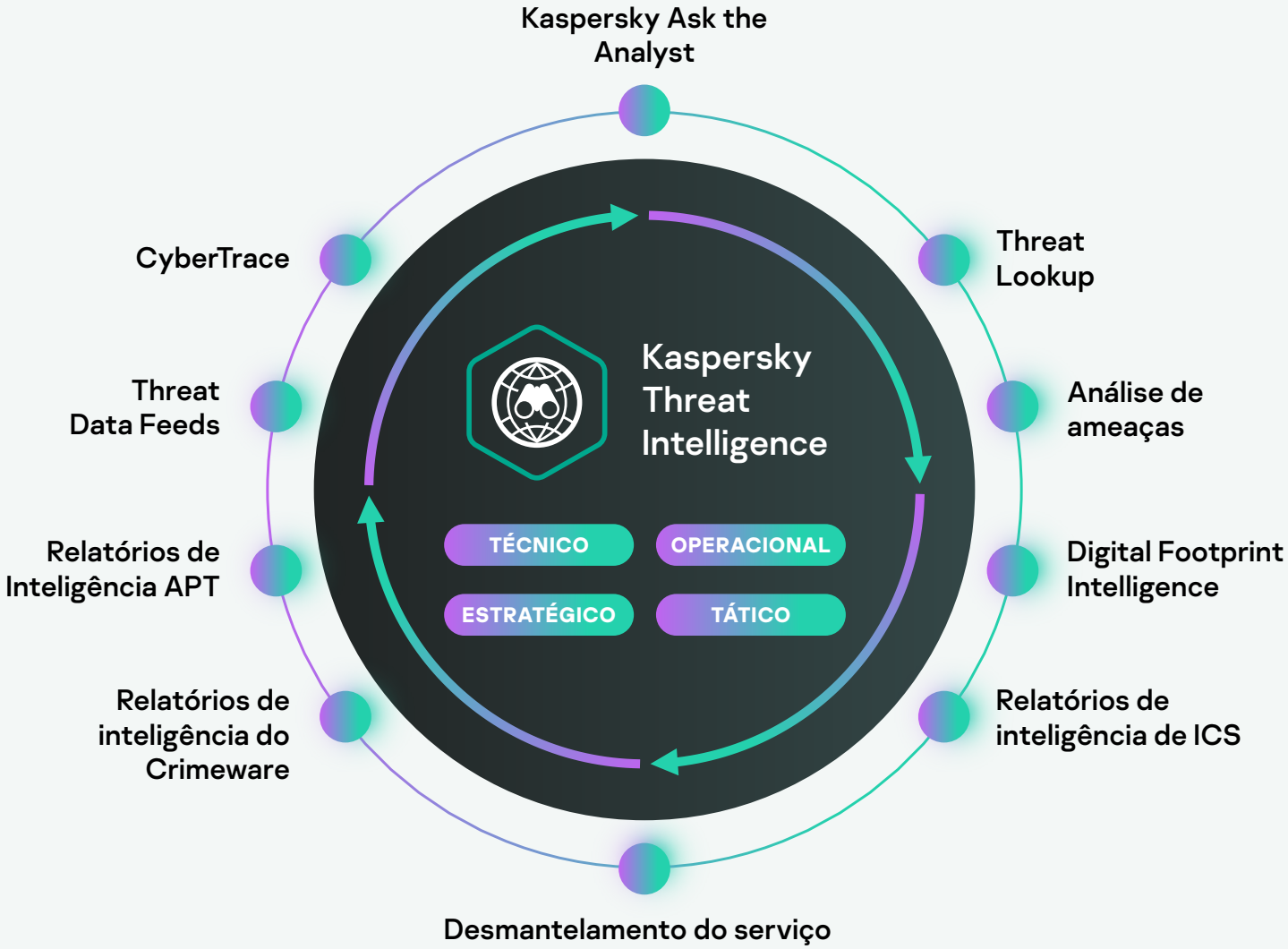
Kaspersky Threat Intelligence

A Threat Intelligence da Kaspersky oferece acesso às informações de que você precisa para mitigar as ameaças virtuais, além de garantir as informações fornecidas pela nossa equipe, de investigadores e analistas, líder em nível mundial.

O conhecimento, a experiência e as informações aprofundadas da Kaspersky sobre todos os aspectos da cibersegurança fizeram com que se tornasse 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 técnica, tática, operacional e estratégica.

O portfólio do Kaspersky Threat Intelligence inclui

Threat Data Feeds, CyberTrace (uma plataforma do Threat Intelligence), Threat Lookup, Threat Analysis (Cloud Sandbox e Cloud Threat Attribution Engine), diversas opções de relatórios do Threat Intelligence e serviços de inteligência de ameaças sob demanda.



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

Kaspersky CyberTrace

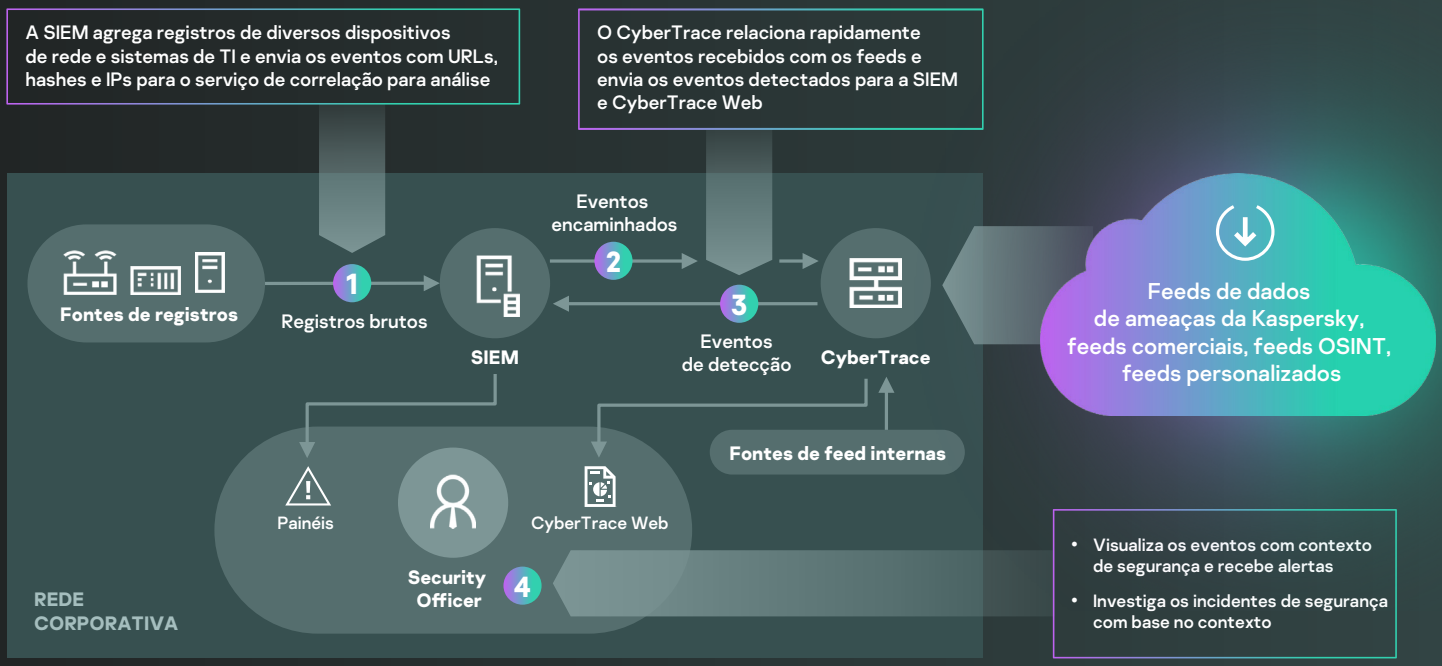
Ao integrar inteligência de ameaças atualizada com leitura por máquinas nos controles de segurança existentes, como sistemas de SIEM, os Centros de Operações de Segurança conseguem automatizar o processo de triagem inicial, fornecendo aos seus analistas de segurança contexto suficiente para identificar imediatamente alertas que precisam ser investigados ou escalados para as equipes de resposta a incidentes para investigação e resposta adicionais. No entanto, o crescimento contínuo no número de feeds de dados de ameaças e fontes de inteligência de ameaças disponíveis torna difícil para as organizações determinar quais informações são relevantes para elas. A inteligência de ameaças é fornecida em diferentes formatos e inclui um grande número de indicadores de comprometimento (IOC), fazendo com que seja difícil para as SIEM ou controles de segurança de rede assimilá-los.

O Kaspersky CyberTrace é uma plataforma de inteligência de 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 (da Kaspersky, de outros fornecedores, OSINT ou de seus próprios feeds de clientes) nos formatos JSON, STIX, XML e CSV e oferece suporte à integração imediata com várias soluções SIEM e fontes de log.

O Kaspersky CyberTrace fornece um conjunto de instrumentos para operacionalizar a inteligência de ameaças de forma excessiva:

- Um banco de dados de indicadores com pesquisa de texto completo e a possibilidade de pesquisar usando consultas de pesquisa avançadas permite pesquisas complexas em todos os campos de indicadores, incluindo campos de contexto
- Páginas com 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.
- Um Gráfico de pesquisa permite explorar visualmente os dados e as detecções armazenadas no CyberTrace e descobrir semelhanças entre as ameaças.
- 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.
- Marcar IoCs simplifica seu gerenciamento. É possível criar uma tag, especificar seu peso (importância) e usá-la para marcar IoCs manualmente. Você também pode classificar e filtrar IoCs com base nessas tags e seus pesos.
- 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.
- Um filtro envia eventos de detecção para soluções SIEM, reduzindo a carga sobre eles e também sobre os analistas
- A multilocação oferece suporte a MSSPs e casos de uso de grandes empresas
- As estatísticas de uso do feed para medição da efetividade dos feeds integrados e a matriz de interseção de feeds ajudam a escolher os fornecedores de inteligência de ameaças mais valiosos
- A HTTP RestAPI permite que você pesquise e gerencie a inteligência de ameaças.

A ferramenta utiliza um processo interno de análise e correspondência de dados de entrada, o que reduz significativamente a carga de trabalho de SIEM. O Kaspersky CyberTrace analisa os registos de entrada e eventos, estabelece rapidamente a correspondência entre os dados resultantes e os feeds, e gera os seus próprios alertas sobre detecção de ameaças. Uma arquitetura de alto nível da integração da solução é apresentada no diagrama abaixo:



Com o Kaspersky CyberTrace e o Kaspersky Threat Data Feeds, os analistas de segurança conseguem:

- Transformar eficazmente e priorizar grandes quantidades de alertas de segurança
- Melhorar e acelerar os processos de triagem e de resposta inicial
- Identificar imediatamente alertas críticos para a empresa e tomar decisões mais informadas sobre os alertas que devem ser escalados para as equipes de IR
- Criar uma defesa proativa e orientada por inteligência

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 ameaças virtuais estão em constante crescimento em termos de frequência, complexidade e ofuscação, à medida que novas tentativas são realizadas para comprometer suas defesas. Os invasores utilizam cadeias de destruição complicadas, e táticas, técnicas e procedimentos (TTP) personalizados nas campanhas para perturbar as suas operações, roubar os seus ativos ou causar danos aos seus clientes.

O Kaspersky Threat Lookup oferece todo o conhecimento adquirido pela Kaspersky sobre ameaças virtuais e respectivas relações, 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 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.

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[1], 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 o seu impacto e frequência. Rastreie e elimine severamente os ataques o mais cedo possível. Quanto antes conseguir descobrir uma ameaça, menos danos são causados, mais rapidamente são efetuadas reparações, e mais cedo as operações de rede podem voltar ao normal

Investigações de incidentes: um gráfico de pesquisas impulsiona as investigações de incidentes permitindo que você explore visualmente dados e detecções armazenadas no Threat Lookup. Ele fornece uma visualização gráfica da relação entre URLs, domínios, IPs, arquivos e outros contextos para que você possa entender melhor todo o escopo de um incidente e identificar sua causa raiz.

Pesquisa principal: pesquise informações em todos os produtos de inteligência ativos contra ameaças e fontes externas (incluindo OSINT IoCs, Dark Web e Internet) em uma interface única e avançada.

Interface Web ou API RESTful fáceis de usar: Use o serviço em modo manual através de uma interface online (através de um navegador Web) ou acesse através de uma API RESTful simples, como você preferir

Vasta gama de formatos de exportação: exporte IOCs (indicadores de comprometimento) ou contexto acionável para formatos de compartilhamento de leitura por máquinas amplamente utilizadas e mais organizadas, como STIX, OpenIOC, JSON, Yara, Snort ou mesmo CSV, para desfrutar da totalidade dos benefícios da inteligência de ameaças, automatizar o fluxo de trabalho das operações ou integrar em controles de segurança como SIEMs.

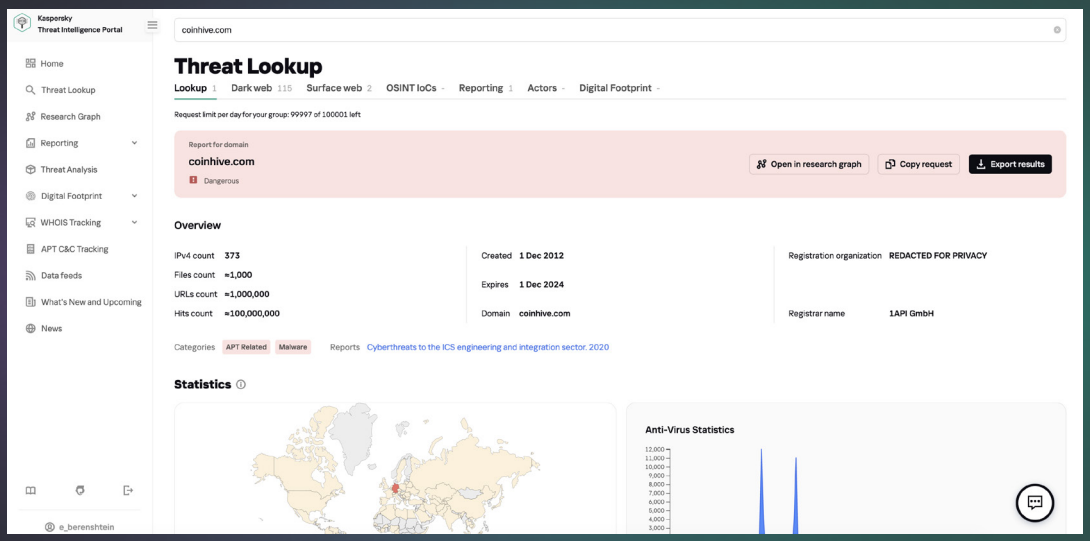
Benefícios

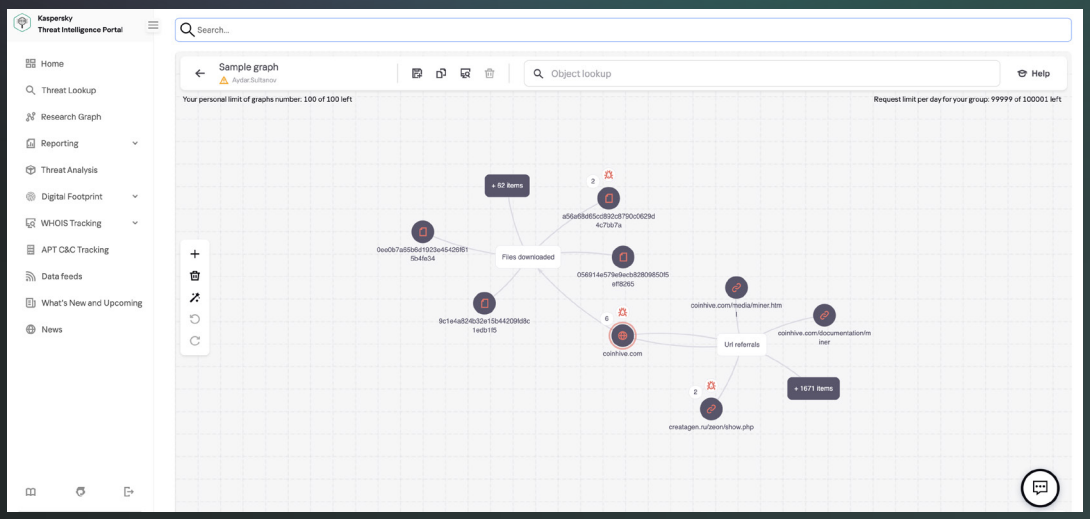
Conduza pesquisas profundas sobre indicadores de ameaças em um contexto altamente validado que permite priorizar ataques e focar na mitigação de ameaças que trazem maior risco ao seu negócio

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

Aprimore sua resposta a incidentes e funcionalidades de busca de ameaças para desfazer a cadeia perigosa antes que sistemas e dados cruciais sejam comprometidos

[1] kaspersky.com.br/top3





Agora você pode

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

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

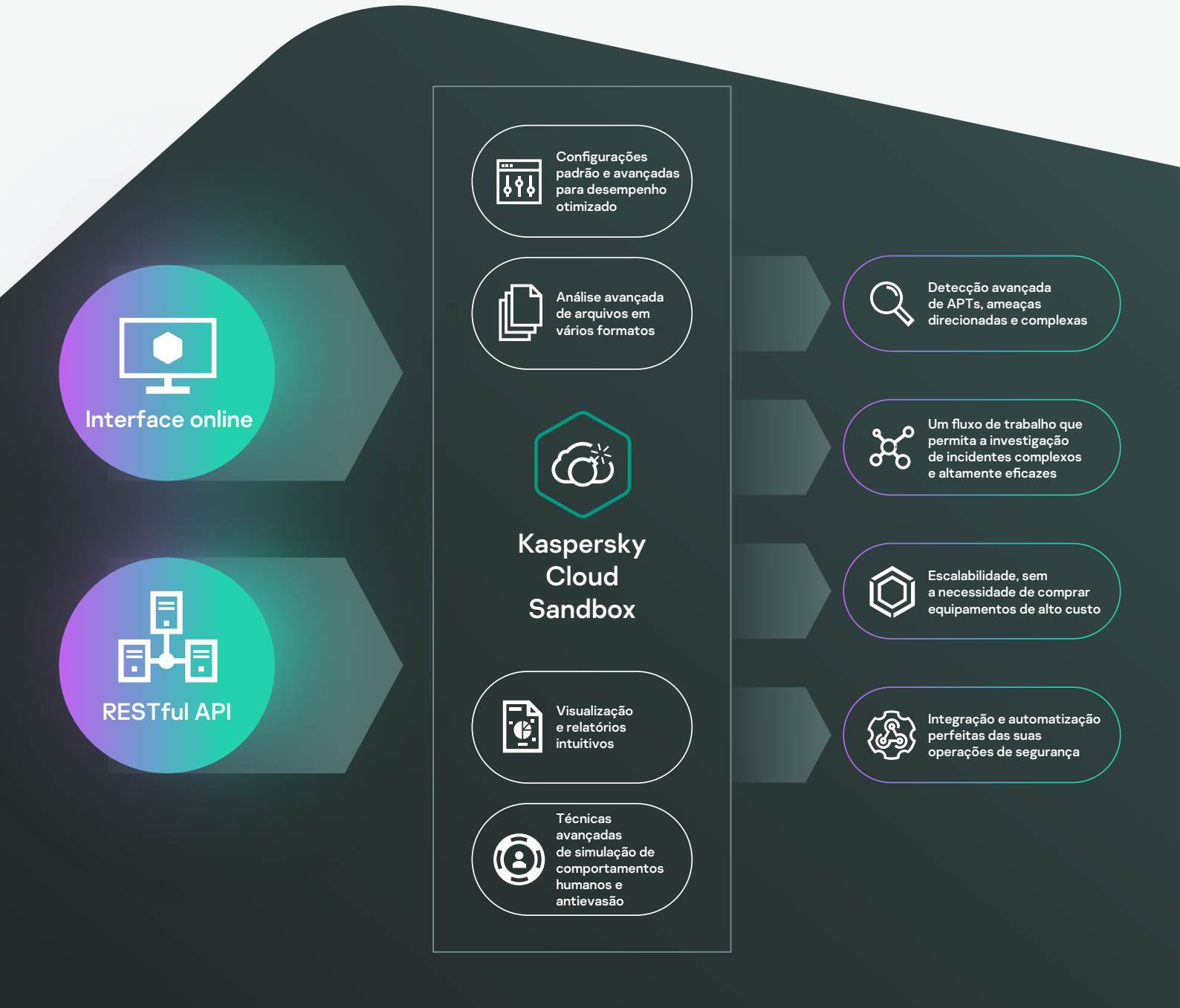
Verificar se o objeto descoberto é comum ou único.

Compreender o motivo pelo qual um objeto deve ser tratado como malicioso.

Kaspersky Cloud Sandbox

É impossível prevenir os ataques direcionados atuais apenas com ferramentas AV tradicionais. O mecanismo dos antivírus conseguem parar apenas as ameaças conhecidas e suas respectivas variações, ao passo que os agentes de ameaças sofisticadas utilizam todos os meios à sua disposição para escapar à detecção automática. As perdas decorrentes de incidentes de segurança da informação continuam aumentando exponencialmente, realçando a importância crescente das capacidades de detecção de ameaças imediata para assegurar uma resposta rápida e combater ameaças antes que ocorram danos significativos.

Tomar uma decisão inteligente com base no comportamento de um arquivo, analisando simultaneamente a memória de processo, a atividade de rede, etc. é a abordagem ideal para compreender as sofisticadas ameaças mais recentes direcionadas e personalizadas. Os dados estatísticos podem ter falta de informação sobre malware modificado, mas as tecnologias de sandbox são ferramentas poderosas que permitem a investigação das origens da amostra de arquivo, a coleta de IOC com base em análise comportamental e a detecção de objetos maliciosos nunca vistos.



Relatórios abrangentes

- DLL carregados e executados
- Ligações externas com nomes de domínio e endereços IP
- Arquivos criados, modificados e eliminados
- Inteligência de ameaças detalhada com contexto acionável para cada indicador de comprometimento (IOC) revelado
- Dumps de memória de processo e dumps de tráfego de rede (PCAP)
- Pedidos e respostas de HTTP e DNS
- Extensões mútuas criadas (mutexes)
- API RESTful
- Chaves de registo modificadas e criadas
- Processos criados pelo arquivo executado
- Capturas de tela
- **e muito mais**

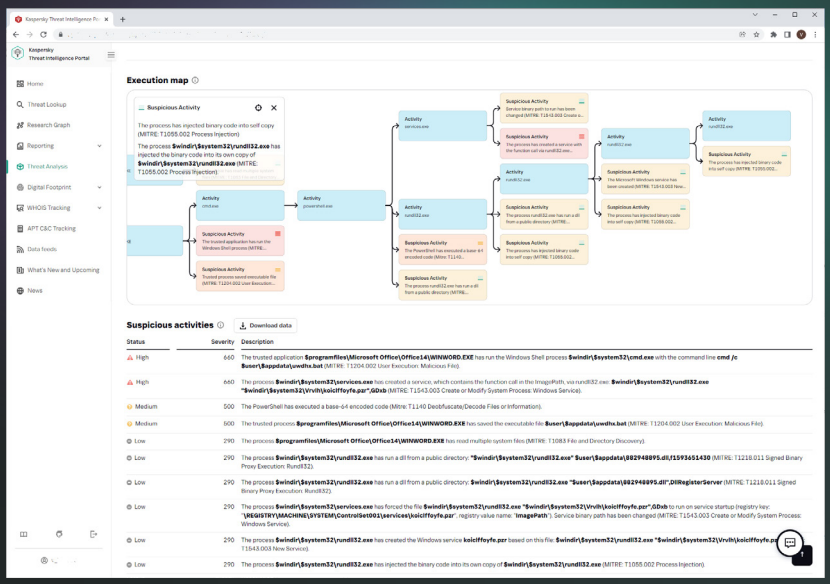
Detecção e mitigação proativa de ameaças

O malware usa diversos métodos para impedir que sua execução seja detectada. Se o sistema não cumprir os parâmetros necessários, o programa malicioso irá muito provavelmente autodestruir-se, sem deixar vestígios. Para o código malicioso ser executado, o ambiente de sandbox tem que conseguir imitar com exatidão o comportamento normal de um usuário final.

O Kaspersky Cloud Sandbox oferece uma abordagem híbrida, que conjuga inteligência de ameaças recolhida a partir de petabytes de dados estatísticos (graças ao Kaspersky Security Network e outros sistemas proprietários), análise comportamental e técnicas antievasão sólidas, com tecnologias que simulam humanos, como clicker automático, percorrer documentos e processos fictícios.

Este produto foi desenvolvido em nosso laboratório de sandbox interno, evoluindo por mais de uma década. A tecnologia incorpora todo nosso conhecimento sobre o comportamento de malware adquirido ao longo de 20 anos de pesquisa contínua de ameaças. Isso nos permite detectar mais de 360 mil novos objetos maliciosos todos os dias para fornecer aos nossos clientes soluções de segurança líder do setor.

Como parte do nosso Threat Intelligence Portal, o Cloud Sandbox é um importante componente do nosso fluxo de trabalho de inteligência de ameaças. Enquanto a pesquisa de ameaças obtém a mais recente inteligência de ameaças detalhada sobre URLs, domínios, endereços IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS, etc., o Cloud Sandbox vincula esse conhecimento com os IOCs gerados pela amostra analisada.



Agora, você pode executar investigações de incidentes altamente eficazes e complexas, obtendo um entendimento imediato da natureza da ameaça, depois fazer associações à medida que pesquisa para revelar os indicadores de ameaça inter-relacionados.

A inspeção pode exigir muitos recursos, especialmente no que se refere a ataques com várias etapas. O Kaspersky Cloud Research Sandbox aumenta sua resposta a incidentes e atividades forenses, fornecendo a você a escalabilidade para processar arquivos automaticamente sem ter que comprar aparelhos caros ou se preocupar com recursos do sistema.

Kaspersky APT Intelligence Reporting

Os clientes do Kaspersky APT Intelligence Reporting recebem acesso contínuo exclusivo às nossas investigações e descobertas, incluindo dados técnicos completos (em vários formatos) sobre cada APT à medida que são descobertos, bem como sobre ameaças que nunca serão divulgadas. Os relatórios contêm um resumo executivo com informações orientadas ao nível C e fáceis de entender que descrevem o APT relacionado, juntamente com uma descrição técnica detalhada do APT com IOCs relacionados e regras YARA para fornecer aos pesquisadores de segurança, analistas de malware, engenheiros de segurança, analistas de segurança de rede e dados acionáveis APT de pesquisadores que permitem uma resposta rápida e precisa à ameaça.

Nossos especialistas também alertam imediatamente sobre qualquer mudança que detectarem nas táticas de grupos de criminosos virtuais. Você também terá acesso ao banco de dados completo de relatórios APT da Kaspersky, outro poderoso componente de pesquisa e análise em suas defesas de segurança.

Benefícios

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.

Informações sobre APTs não públicos
Por várias razões, nem todas as ameaças de alto nível são divulgadas ao público em geral. Mas nós compartilhamos todos eles com nossos clientes

Acesso privilegiado
Receba descrições técnicas sobre as ameaças mais recentes durante as investigações em andamento, antes de serem divulgadas ao público em geral

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

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

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

Monitoramento contínuo de campanhas de APT
Acesso a inteligência acionável durante a investigação com informações sobre distribuição de APTs, IOCs, infraestruturas de comando e controle etc.

API RESTful
Integração e automação perfeitas dos seus fluxos de trabalho de segurança

Kaspersky Digital Footprint Intelligence

À medida que a sua empresa cresce, a complexidade e a distribuição dos seus ambientes de TI crescem também, criando um desafio: proteger sua presença digital amplamente 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 as suas mudanças e reagir a informações atualizadas sobre ativos digitais expostos.

As organizações utilizam uma vasta gama de ferramentas de segurança nas suas operações de segurança, mas continuam existindo ameaças digitais que causam preocupação, como: capacidades para detectar e mitigar atividades internas, planos e esquemas de ataque de criminosos virtuais localizados nos fóruns da Dark Web, etc. Para ajudar os analistas de segurança a explorar a visão do adversário sobre os recursos da sua empresa, descobrir prontamente os potenciais vetores de ataque a sua disposição e ajustar as defesas de acordo, a Kaspersky criou o Kaspersky Digital Footprint Intelligence.

Qual a melhor maneira de lançar um ataque contra sua organização? Qual a maneira com melhor custo-benefício para atacar você? Quais informações estão disponíveis para um invasor que tenha sua empresa como alvo? Sua infraestrutura já foi comprometida sem seu conhecimento?

O Kaspersky Digital Footprint Intelligence responde a estas e a outras questões à medida que nossos especialistas reúnem um panorama abrangente do seu status de ataque, identificando os pontos fracos prontos para serem explorados e revelando evidências de ataques passados, atuais e até planejados.

O produto oferece:

- Inventário do perímetro de rede utilizando métodos não intrusivos para identificar os recursos da rede do cliente e os serviços expostos, que são um potencial ponto de entrada para um ataque, como interfaces de gerenciamento deixadas não intencionalmente no perímetro ou serviços mal configurados, interfaces de dispositivos, etc.
- 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).
- Identificação, monitoramento e análise de quaisquer ataques direcionados ativos ou ataques que estejam sendo planejados, campanhas de APT direcionadas para à sua empresa, setor ou região de operações.
- Identificação de ameaças direcionadas a seus clientes, parceiros e assinantes, cujos respectivos sistemas infectados poderiam então ser usados para o atacar.
- Monitoramento discreto de sites pastebin, fóruns públicos, blogs, canais de mensagens instantâneas, comunidades e fóruns online clandestinos restritos para descobrir contas comprometidas, vazamentos de informações ou ataques contra sua organização que estejam em discussão ou planejamento.

Destaques

O Kaspersky Digital Footprint Intelligence usa técnicas OSINT combinadas com análises automatizadas e manuais da Internet, Deep e Dark Web, além da base de conhecimento interna da Kaspersky para fornecer insights e recomendações acionáveis.

O produto está disponível no Kaspersky Threat Intelligence Portal. Você pode adquirir quatro relatórios trimestrais com alertas anuais de ameaças em tempo real ou adquirir um único relatório com alertas ativos por seis meses.

Pesquise na internet e na Dark Web informações quase em tempo real sobre eventos de segurança global que estão ameaçando seus ativos, bem como dados confidenciais expostos em comunidades e fóruns clandestinos restritos. A licença anual inclui 50 pesquisas por dia em fontes externas e na base de conhecimento da Kaspersky.

O Kaspersky Digital Footprint Intelligence cria uma solução única com o Kaspersky Takedown Service. A licença anual inclui 10 solicitações para derrubar domínios maliciosos e de phishing por ano.

Inventário de perímetro de rede (incluindo nuvem)

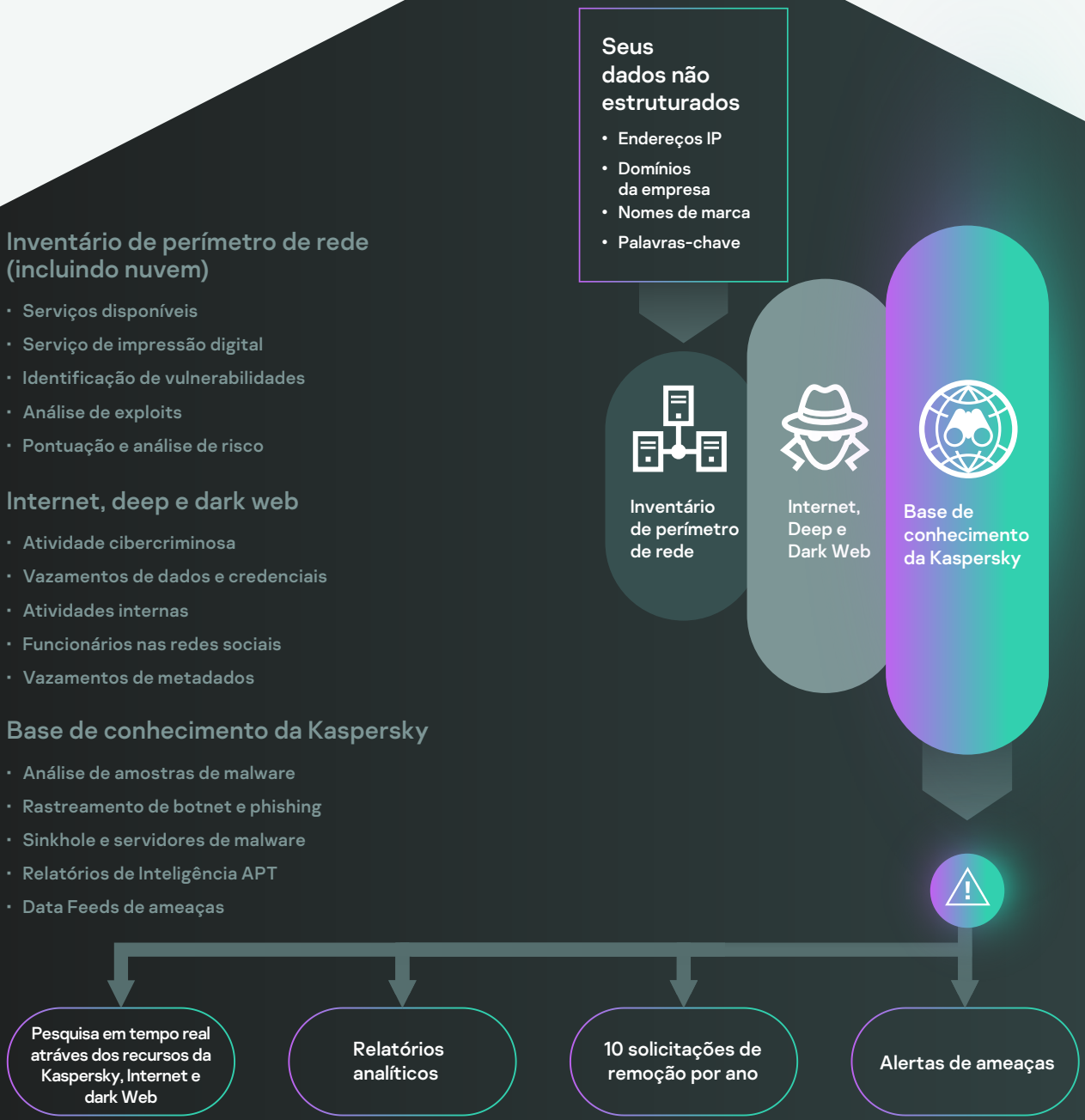
- Serviços disponíveis
- Serviço de impressão digital
- Identificação de vulnerabilidades
- Análise de exploits
- Pontuação e análise de risco

Internet, deep e dark web

- Atividade cibercriminosa
- Vazamentos de dados e credenciais
- Atividades internas
- Funcionários nas redes sociais
- Vazamentos de metadados

Base de conhecimento da Kaspersky

- Análise de amostras de malware
- Rastreamento de botnet e phishing
- Sinkhole e servidores de malware
- Relatórios de Inteligência APT
- Data Feeds de ameaças



Relatórios do Kaspersky ICS Threat Intelligence

O Kaspersky 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. Os relatórios são entregues através de um portal baseado na Web, o que significa que você pode começar a utilizar o serviço imediatamente.

Relatórios incluídos em sua assinatura

1. **Relatórios de APT.** Relatórios sobre novas APT e campanhas de ataque de alto volume que visam organizações industriais, e atualizações sobre ameaças ativas.
2. **O panorama de ameaças.** Relatórios sobre mudanças significativas no cenário de ameaças para sistemas de controle industriais, fatores críticos recém-descobertos que afetam os níveis de segurança de ICS e a exposição dos ICS a ameaças, incluindo informação específica da região, do país e do setor.
3. **Vulnerabilidades encontradas.** Relatórios sobre vulnerabilidades identificadas pela Kaspersky nos mais populares produtos utilizados nos sistemas de controle industrial, a internet das coisas industrial e infraestruturas em várias indústrias.
4. **Análise e mitigação de vulnerabilidade.** Os nossos consultores fornecem recomendações acionáveis de especialistas da Kaspersky para ajudar a identificar e mitigar vulnerabilidades na sua infraestrutura.

Com a inteligências de ameaças, você pode

Detectar e bloquear

ameaças reportadas para proteger ativos críticos, incluindo componentes de software e hardware, e assegurar a segurança e a continuidades de processos tecnológicos

Correlacionar

qualquer atividade maliciosa e suspeita que você detectar em ambientes industriais com os resultados de pesquisa da Kaspersky para atribuir sua detecção à campanha maliciosa em questão, identificar ameaças e responder prontamente a incidentes

Realizar

uma avaliação de vulnerabilidade dos seus ativos e ambientes industriais com base em avaliações precisas do escopo e a gravidade da vulnerabilidade, para tomar decisões informadas sobre o gerenciamento de correções ou a implementar outras medidas preventivas recomendadas pela Kaspersky

Tire proveito de

informações sobre tecnologias, táticas e procedimentos de ataque, vulnerabilidades recém-descobertas e outras mudanças importantes no cenário de ameaças para:

- Identificar e avaliar os riscos das ameaças comunicadas e de outras ameaças semelhantes
- Planejar e projetar alterações na infraestrutura industrial para assegurar a segurança da produção e continuidade do processo tecnológico
- Realizar atividades de conscientização de segurança com base na análise de casos reais para criar cenários de treinamento personalizados e planejar exercícios de equipe vermelha X equipe azul
- Tomar decisões estratégicas informadas para investir em cibersegurança e para assegurar a resiliência das operações

Kaspersky Ask the Analyst

Cibercriminosos estão constantemente desenvolvendo formas sofisticadas de atacar empresas. O cenário de ameaças em constante transição e de rápido crescimento da atualidade demonstram o uso de técnicas de crimes cibernéticos cada vez mais ágeis. As organizações enfrentam incidentes complexos causados por ataques não-malware, sem arquivo, 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.

Pesquisa contínua de ameaças

permite que a Kaspersky descubra, se infiltre e monitore comunidades fechadas e fóruns clandestinos em todo o mundo frequentados por cibercriminosos. Nossos analistas tiram proveito desse acesso para detectar e investigar proativamente as ameaças mais prejudiciais e famosas, bem como ameaças projetadas para organizações específicas.

Em uma época dominada por ciberataques rondando empresas, 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 poder recorrer à assistência especializada de terceiros.** A experiência externa pode esclarecer os caminhos prováveis de ataques complexos e APTs, e fornecer conselhos acionáveis sobre a maneira mais decisiva de eliminá-los.

Serviços do Ask the Analyst

(Assinatura unificada baseada sob demanda)

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. 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.

APT e Crimeware

Informações adicionais sobre relatórios publicados e pesquisas em andamento (além do serviço APT ou Crimeware Intelligence Reporting)[1]

Análise de malware

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

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)

Inteligência da Dark Web[2]

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

Solicitações relacionadas ao 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

[1] Disponível apenas para clientes com serviço de Relatórios Ativos de Inteligência APT e/ou Crimeware

[2] Já incluído na assinatura do Kaspersky Digital Footprint Intelligence

Benefícios do serviço

Incremente sua expertise

Tenha acesso sob demanda a especialistas do setor, sem ter que perder tempo procurando e sem investir em especialistas contratados em tempo integral

Agilize a 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 conhecidos

Como funciona?

O Kaspersky Ask the Analyst pode ser comprado separadamente ou acrescentado a qualquer um de nossos serviços de inteligência contra ameaças.

Você pode solicitar diretamente da sua Conta Corporativa Kaspersky, no nosso portal de suporte ao cliente corporativo. Responderemos por e-mail, mas se necessário e acordado com você, podemos organizar 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 do serviço:

- Esclareça todos os detalhes em relatórios de inteligência contra ameaças publicados anteriormente
- Obtenha informações adicionais para IoCs já fornecidos
- Obtenha detalhes sobre vulnerabilidades e recomendações sobre como proteger-se contra exploits
- Obtenha detalhes adicionais sobre as atividades específicas da Dark Web de seu interesse
- 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
- Priorize efetivamente alertas/ incidentes com informações contextuais detalhadas, além de categorização para IoCs relacionados fornecidas por meio de relatórios sintéticos
- Solicite assistência para identificação, caso seja detectada alguma atividade incomum relacionada com um APT ou um agente de crimeware
- Envie arquivos de malware para análise abrangente para compreender o comportamento e a funcionalidade das amostras fornecidas

Amplie conhecimentos 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 aumentar suas capacidades atuais com nosso conhecimento e recursos exclusivos.

Kaspersky Takedown Service

Desafio

Os cibercriminosos criam domínios maliciosos e de phishing que são usados para atacar sua empresa e suas marcas. A incapacidade de mitigar rapidamente essas ameaças uma vez identificadas, pode levar a perda de receita, danos à marca, perda de confiança do cliente, vazamentos de dados e muito mais. Mas gerenciar remoções desses domínios é um processo complexo que requer experiência e tempo.

Solução

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 on-line e reputação, trabalhando com organizações internacionais, agências nacionais e regionais de aplicação da lei (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.

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 recurso solicitado seja removido com sucesso.

Proteção sem esforço

O Kaspersky Takedown Service mitiga 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.

Benefícios do serviço

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.

Gerenciamento de ponta a ponta

Gerenciaremos todo o processo de remoção e minimizaremos seu envolvimento.

Visibilidade completa

Você será notificado em cada etapa do processo, desde o registro da sua solicitação até a remoção bem-sucedida.

Integração com Digital Footprint Intelligence

O serviço se integra ao Kaspersky Digital Footprint Intelligence, que fornece notificações em tempo real sobre domínios de phishing e malware, projetados para danificar, abusar ou se passar por sua marca/organização. Uma solução única é um componente importante de uma estratégia abrangente de cibersegurança.

Principais benefícios

- Permite a visibilidade global de ameaças, a detecção oportuna de ameaças virtuais, a priorização de alertas de segurança e uma resposta eficaz a incidentes de segurança da informação
- Poupa seus analistas e ajuda a focar sua força de trabalho em ameaças reais
- 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
- 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

Conclusão

Combater as ciberameaças atuais requer uma visão de 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 da Kaspersky trabalhamos para oferecer suporte aos nossos clientes com a mais recente inteligência de ameaças de todo o mundo, ajudando-os a manter sua imunidade até mesmo contra ciberataques nunca vistos.

FORRESTER®

A Kaspersky foi reconhecida como Líder no Forrester Wave: External Threat Intelligence Services, 2021

www.kaspersky.com.br