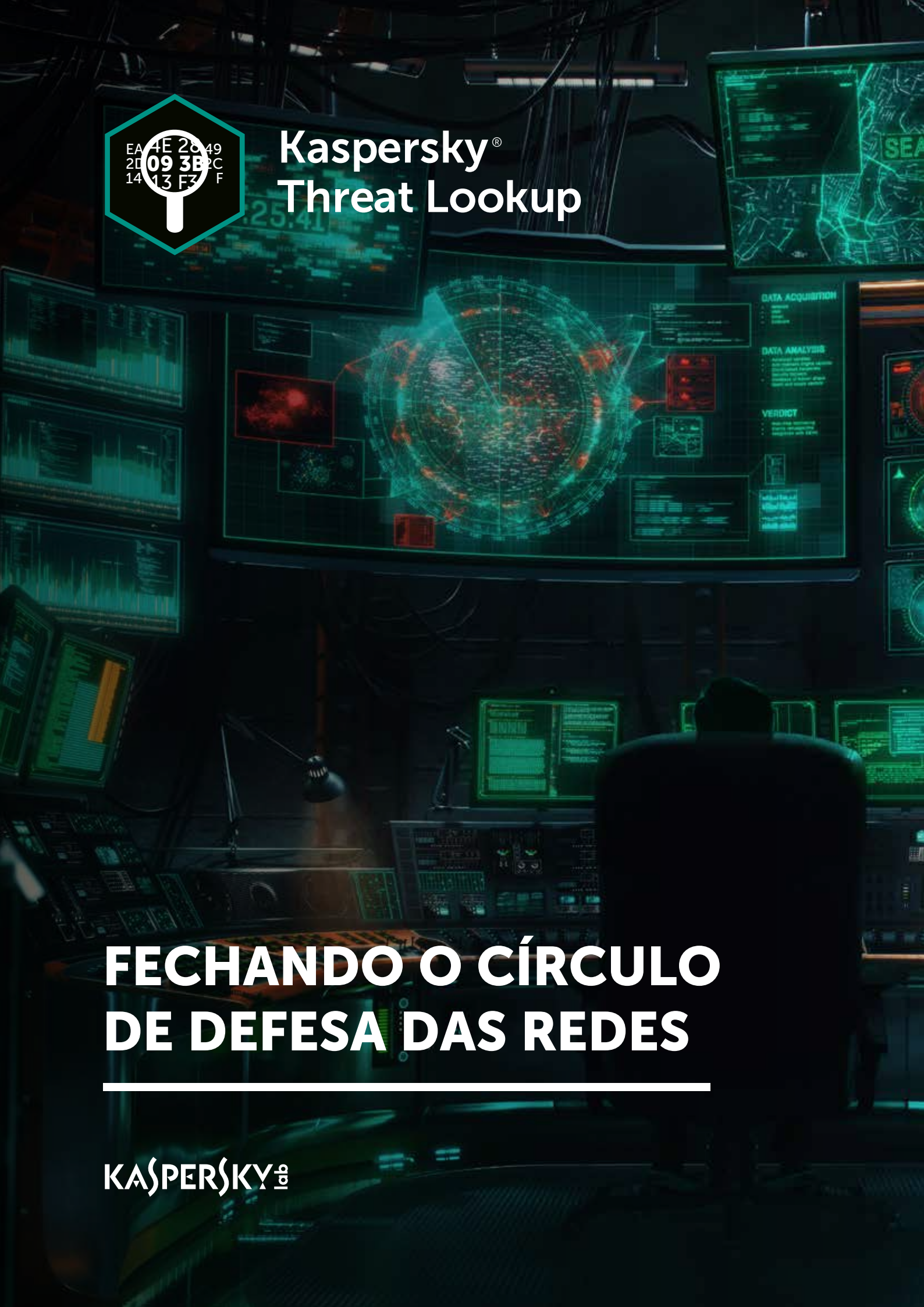


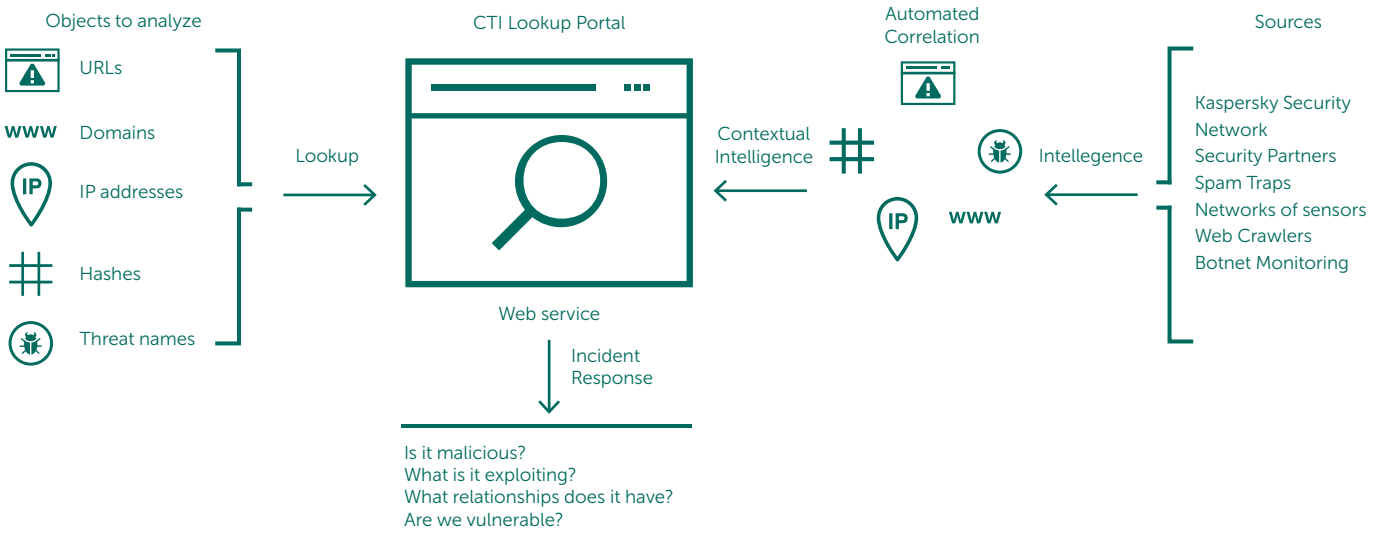
FECHANDO O CÍRCULO DE DEFESA DAS REDES

KASPERSKY lab

Nos dias de hoje, os crimes virtuais não têm fronteiras e os recursos técnicos são aprimorados rapidamente: temos visto ataques cada vez mais sofisticados, com os criminosos virtuais usando recursos do mercado negro na Web para ameaçar seus alvos. A frequência, a complexidade e a ofuscação das ameaças virtuais aumentam constantemente, à medida que são feitas novas tentativas de comprometer as suas defesas. Os invasores estão usando kill chains complicadas, assim como táticas, técnicas e procedimentos (TTPs, Tactics, Techniques and Procedures) personalizados nas campanhas para interromper seus negócios, roubar seus recursos ou prejudicar seus clientes.

O acesso ao Kaspersky Threat Lookup oferece inteligência confiável e imediata sobre ameaças virtuais, objetos legítimos, suas interconexões e indicadores, com contexto prático para informar sua empresa ou seus clientes sobre os riscos e as implicações associados. Agora você pode atenuar e responder às ameaças com mais eficiência, defendendo-se contra os ataques antes mesmo que eles aconteçam.

O Kaspersky Threat Lookup oferece todo o conhecimento adquirido pela Kaspersky Lab sobre ameaças virtuais e suas relações, reunindo tudo isso em um serviço Web avançado. O objetivo é fornecer às suas equipes de segurança o máximo de dados possível, impedindo os ataques virtuais antes que eles afetem a organização. A plataforma recupera as informações detalhadas de ameaças mais recentes referentes a URLs, domínios, endereços IP, hashes de arquivos, nomes de ameaças, dados estatísticos e comportamentais, dados de WHOIS/DNS, etc. O resultado é a visibilidade global de ameaças novas e emergentes, que ajuda a proteger sua organização e auxilia na resposta a incidentes.



Recursos:

- **Informações confiáveis:** Um atributo importante do Kaspersky Threat Lookup é a confiabilidade dos nossos dados de inteligência de ameaças, enriquecidos com contexto prático. Os produtos da Kaspersky Lab são líderes de mercado em testes de antimalware1, demonstrando a qualidade inigualável da nossa inteligência de ameaças ao oferecer as mais altas taxas de detecção, com falsos positivos próximos de zero.
- **Altos níveis de cobertura em tempo real:** A inteligência de ameaças é gerada automaticamente em tempo real, com base em resultados do mundo todo (graças à Kaspersky Security Network, que mostra informações de uma porcentagem considerável de todo o tráfego da Internet e de todos os tipos de dados, cobrindo dezenas de milhões de usuários finais em mais de 213 países) com altos níveis de cobertura e precisão.
- **Busca de ameaças:** Seja proativo na prevenção, detecção e resposta a ataques para minimizar o impacto e a frequência deles. Rastreie e elimine os ataques ativamente tão logo quanto possível. Quanto antes você descobrir uma ameaça, menos danos serão causados, mais rápido serão feitos os reparos e mais cedo as operações de rede poderão voltar ao normal.
- **Dados ricos:** A inteligência de ameaças do Kaspersky Threat Lookup abrange uma imensa gama de tipos de dados, inclusive hashes, URLs, IPs, whois, pDNS, GeoIP, atributos de arquivos, dados estatísticos e comportamentais, cadeias de download, carimbos de data/hora, entre outros. Com esses dados, você pode avaliar o cenário diversificado de ameaças de segurança que está enfrentando.
- **Disponibilidade contínua:** A inteligência de ameaças é gerada e monitorada por uma infraestrutura altamente tolerante a falhas, garantindo a disponibilidade contínua e um desempenho consistente.
- **Revisão periódica por especialistas em segurança:** Centenas de especialistas, inclusive analistas de segurança de todas as partes do mundo, especialistas em segurança da nossa GReAT Team conhecidos no mundo inteiro e equipes de P&D de ponta, tudo contribui para gerar informações valiosas sobre ameaças. reais.

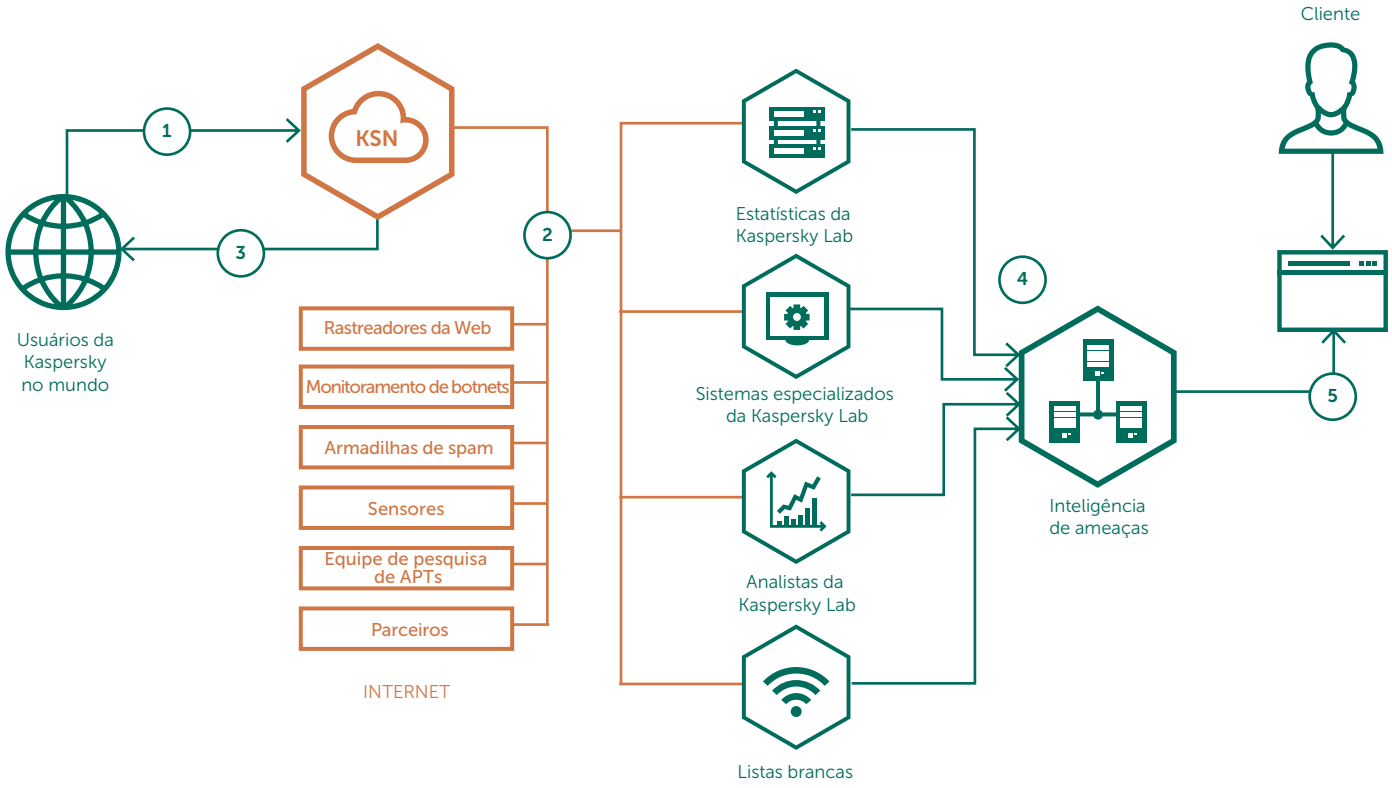
- **Análise de área restrita:**[2] Detecte ameaças desconhecidas executando objetos suspeitos em um ambiente seguro e examine todo o escopo de comportamento de ameaças e os artefatos em relatórios fáceis de compreender.
- **Ampla gama de formatos de exportação:** Exporte indicadores de comprometimento (IOCs, Indicators of Compromise) ou contexto prático para formatos de compartilhamento de leitura por máquina mais organizados e amplamente usados, como STIX, OpenIOC, JSON, Yara, Snort ou até mesmo CSV, e aproveite todos os benefícios da inteligência de ameaças, automatize o fluxo de trabalho das operações ou faça a integração com controles de segurança, como SIEMs.
- **Interface Web ou API RESTful fáceis de usar:** Use o serviço em modo manual por meio de uma interface Web. (via navegador) ou acesse por meio de uma API RESTful simples, conforme sua preferência.
- **Pesquisa inversa de WHOIS:** Pesquise domínios e endereços IP necessários definindo critérios específicos nos dados de WHOIS (por exemplo, contato do domínio, data de criação, etc.).
- **Rastreamento de WHOIS:** Envie campos específicos de dados de WHOIS para a pesquisa regular e automática dos registros WHOIS que atendem aos seus critérios. Notificações por e-mail sobre novos registros no banco de dados de WHOIS que atendem aos critérios de pesquisa são enviadas automaticamente para os destinatários desejados.

Principais benefícios:

- **Melhore e acelere os recursos de resposta a incidentes e perícia fornecendo às equipes de segurança/**SOC informações relevantes sobre ameaças e dados globais sobre o que está por trás dos ataques direcionados. Diagnostique e analise incidentes de segurança em hosts e na rede com mais eficiência e eficácia, e priorize os sinais de sistemas internos contra ameaças desconhecidas, minimizando o tempo de resposta a incidentes e interrompendo a kill chain antes que dados e sistemas essenciais sejam comprometidos.
- **Faça buscas detalhadas nos indicadores de ameaças,** como endereços IP, URLs, domínios ou hashes de arquivos, com contexto de ameaças altamente validado, o que permite priorizar ataques, melhorar as decisões sobre pessoal e alocação de recursos, e se concentrar em atenuar as ameaças que representam mais risco para os seus negócios.
- **Atenue os ataques direcionados.** Aprimore sua infraestrutura de segurança com informações táticas e estratégicas de ameaças, adaptando as estratégias de defesa para combater as ameaças enfrentadas pela sua organização

Fontes de inteligência de ameaças:

A inteligência de ameaças é obtida por meio de uma fusão de fontes heterogêneas e altamente confiáveis, como a Kaspersky Security Network (KSN) e nossos rastreadores da Web, nosso serviço de monitoramento de botnets (monitoramento de botnets e seus alvos e atividades, 24 horas por dia, 7 dias por semana, 365 dias por ano), armadilhas de spam, equipes de pesquisa, parceiros e outros dados históricos sobre objetos maliciosos coletados pela Kaspersky Lab durante quase duas décadas. Depois, em tempo real, todos os dados agregados são cuidadosamente inspecionados e refinados através de diversas técnicas de pré-processamento, como critérios estatísticos, sistemas especializados da Kaspersky Lab (áreas restritas, mecanismos de heurística, ferramentas de análise de similaridade, perfis comportamentais etc.), validação por analistas e verificação de lista branca.



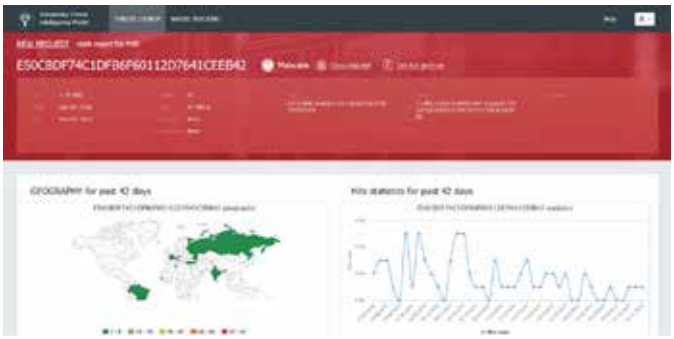
A inteligência de ameaças da Kaspersky abrange dados de indicadores de ameaças avaliados detalhadamente, obtidos do mundo real em tempo real.

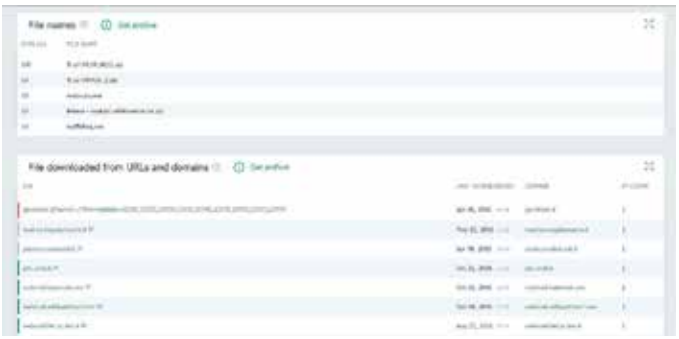
[2]. O lançamento do recurso deve acontecer no primeiro semestre de 2017.

Agora é possível:

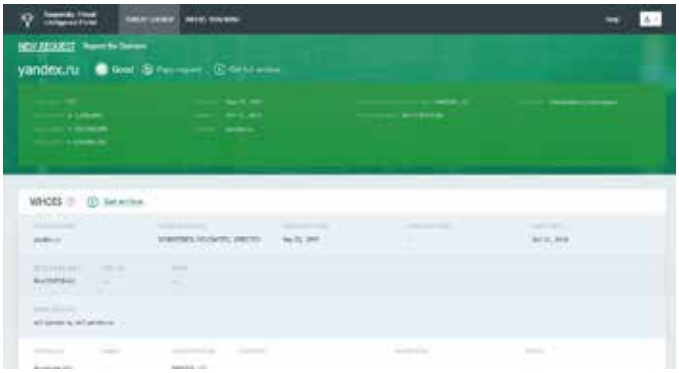
- Pesquisar indicadores de ameaças usando uma interface Web ou a API RESTful.
- Entender por que um objeto deve ser considerado malicioso.
- Verificar se o objeto descoberto se alastrou ou é único.
- Examinar detalhes avançados, como certificados, nomes comuns, caminhos de arquivos ou URLs relacionados para descobrir novos objetos suspeitos.

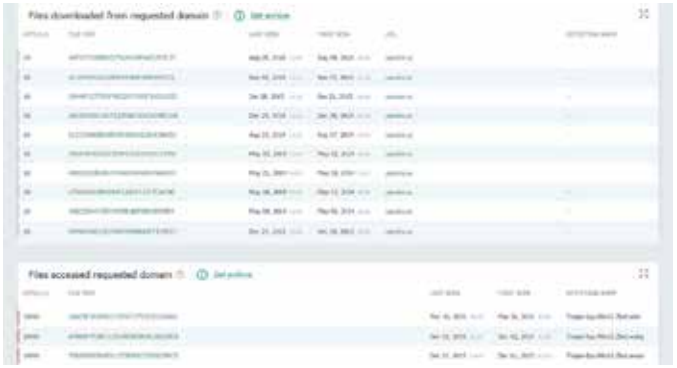
Esses são apenas exemplos. Existem inúmeras formas de aproveitar essa fonte rica e contínua de dados de inteligência relevantes e granulares.





Saiba quem são seus inimigos e seus amigos. Reconheça arquivos, URLs e endereços IP comprovadamente não maliciosos, acelerando as investigações. Quando cada segundo pode ser crucial, não perca um tempo precioso analisando objetos confiáveis.





Nossa missão é proteger o mundo de todos os tipos de ameaças virtuais. Para isso, e para tornar a Internet segura e protegida, é fundamental compartilhar e ter acesso a informações de ameaças em tempo real. O acesso oportuno a essas informações é muito importante para a proteção eficiente de seus dados e suas redes. Agora o Kaspersky Threat Lookup torna o acesso a essas informações mais eficiente e simples do que nunca.

Para obter mais informações sobre o Kaspersky Threat Lookup ou qualquer de nossos serviços de inteligência de segurança, envie um e-mail para intelligence@kaspersky.com

KASPERSKY lab

O PODER
DA PROTEÇÃO