kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

O número de alertas de segurança processados por analistas de segurança de informação todos os dias está crescendo exponencialmente. Com a análise dessa quantidade de dados, a triagem, a validação e a priorização eficazes de alertas são praticamente impossíveis. Há vários sinais de alerta vindos de inúmeros produtos de segurança, que fazem com que alertas importantes fiquem perdidos no ruído, resultando em sobrecarga dos analistas. Ferramentas de análise de segurança, gestão de registros e SIEMs que agregam dados de segurança e correlacionam alarmes correspondentes ajudam a reduzir o número de alertas, garantindo verificação adicional, mas os analistas de segurança continuam extremamente sobrecarregados.

A inteligência de ameaças é fornecida em diferentes formatos e inclui muitos indicadores de comprometimento (IoCs), fazendo com que seja difícil para as SIEMs ou para os controles de segurança de rede assimilá-los.

Permitir a triagem e a análise de alertas de forma eficaz

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 muitos indicadores de comprometimento (IoCs), fazendo com que seja difícil para as SIEMs ou para os 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 nos formatos JSON, STIX, XML e CSV que você queira usar (feeds de inteligência de ameaças da Kaspersky, outros fornecedores, OSINT ou feeds personalizados), e oferece suporte à integração pronta para uso com várias soluções de SIEM e fontes de registro.

O Kaspersky CyberTrace utiliza um processo interno de análise e correspondência de dados de entrada, o que reduz significativamente a carga de trabalho de SIEM. Ele analisa os registros 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 na Figura abaixo:

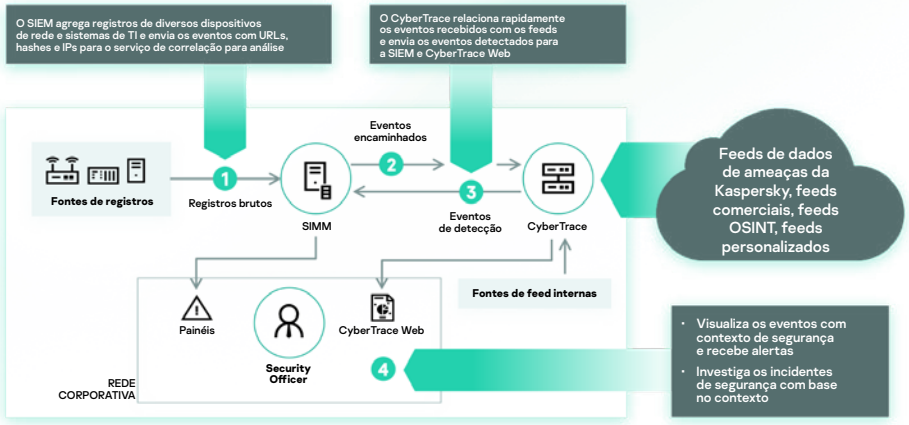


Figura 1. Esquema de integração do Kaspersky CyberTrace

Recursos do produto

O Kaspersky CyberTrace fornece um conjunto de instrumentos para operacionalizar a inteligência de ameaças a fim de realizar uma triagem de alertas e resposta inicial eficazes:

- 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. A filtragem de resultados por fornecedor de inteligência simplifica o processo de análise da inteligência de ameaças.
- 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, de modo que os analistas podem discutir ameaças nos comentários e adicionar inteligência de ameaças internas sobre o indicador. Se o indicador foi detectado, as informações sobre as datas de detecção e os links para a lista de detecções ficarão disponíveis.

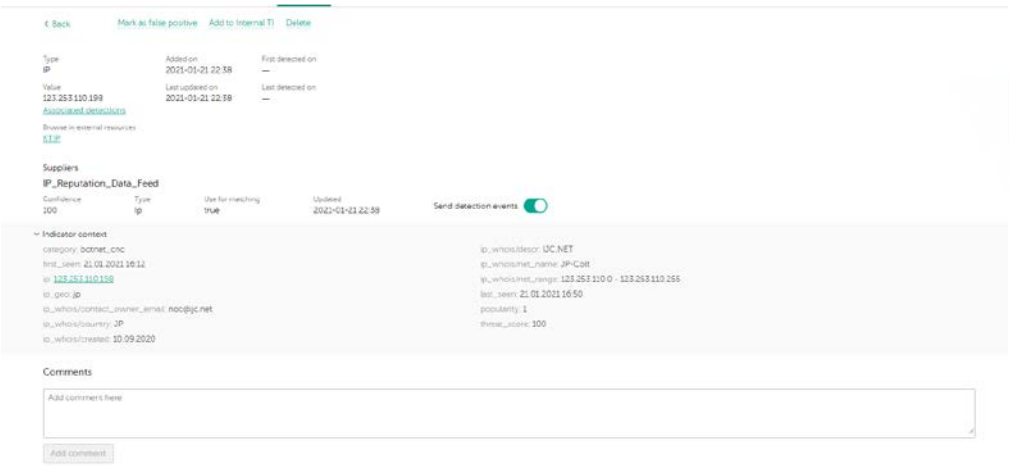


Figura 2. Informações detalhadas sobre um indicador provenientes de todos os fornecedores de inteligência de ameaças

- **Um gráfico de pesquisa permite explorar visualmente os dados e as detecções armazenadas no CyberTrace e descobrir semelhanças entre as ameaças. Ele permite a visualização gráfica da relação entre URLs, domínios, IPs, arquivos e outros contextos encontrados durante investigações. O gráfico inclui os seguintes recursos: transformações, minigráfico, agrupamento de endpoint, adição de links de maneira manual, adição de indicadores e pesquisa por endpoints no gráfico.**

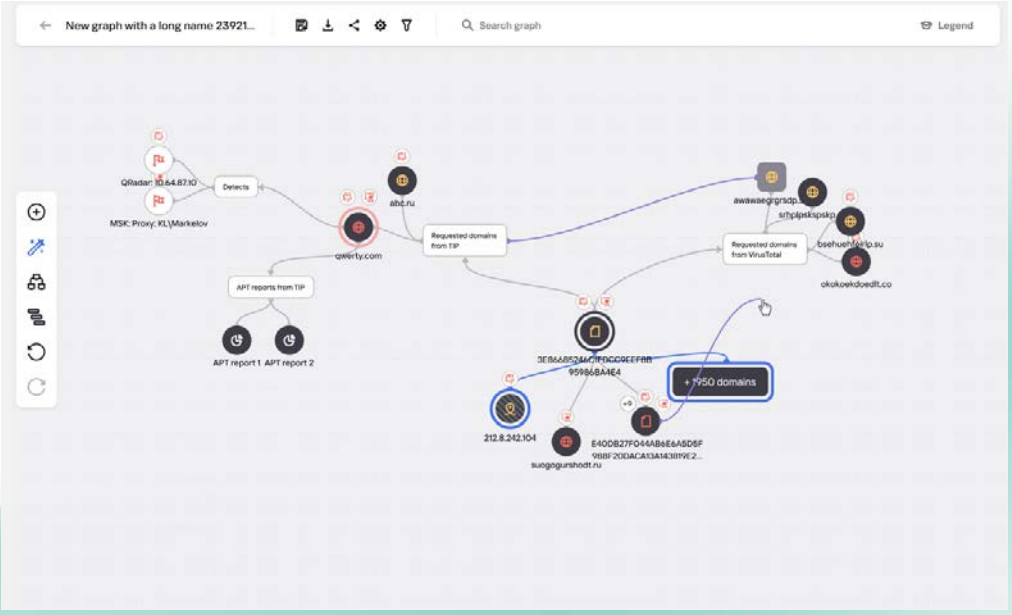


Figura 3. Gráfico de pesquisa

- O recurso de exportação de indicadores é compatível com 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.

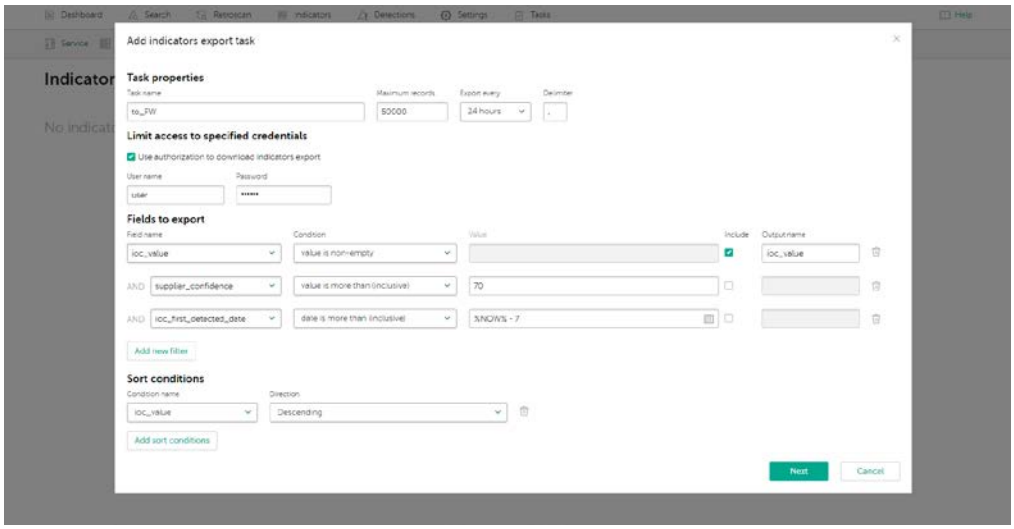


Figura 4. Tarefa de exportação de indicadores

- 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.

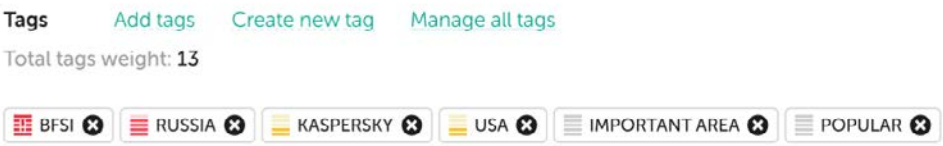


Figura 5. Tags de IoC

- Com o recurso de correlação histórica (retroscan), é possível analisar itens a partir de eventos verificados anteriormente usando os feeds mais recentes para encontrar ameaças previamente descobertas. Todas as detecções históricas são incluídas no relatório para investigação futura.
- Um filtro para enviar eventos de detecção a soluções de SIEM reduz a carga sobre eles e sobre os analistas que enfrentam a fadiga de alertas. Ele permite que você envie ao SIEM apenas as detecções mais perigosas, aquelas que devem ser tratadas como incidentes. Todas as demais detecções ficam salvas no banco de dados interno e podem ser usadas durante análises de causa ou para descoberta de ameaças.
- A multilocação é compatível com casos de uso de empresas que fornecem serviços gerenciados de segurança (MSSP) ou de grandes empresas quando um provedor de serviços (escritório central) precisa lidar separadamente com eventos de diferentes filiais (locações). Dessa forma, apenas uma instância do Kaspersky CyberTrace pode ser conectada a diferentes soluções de SIEM a partir de diferentes locações, e você pode configurar quais feeds devem ser usados com cada uma delas.

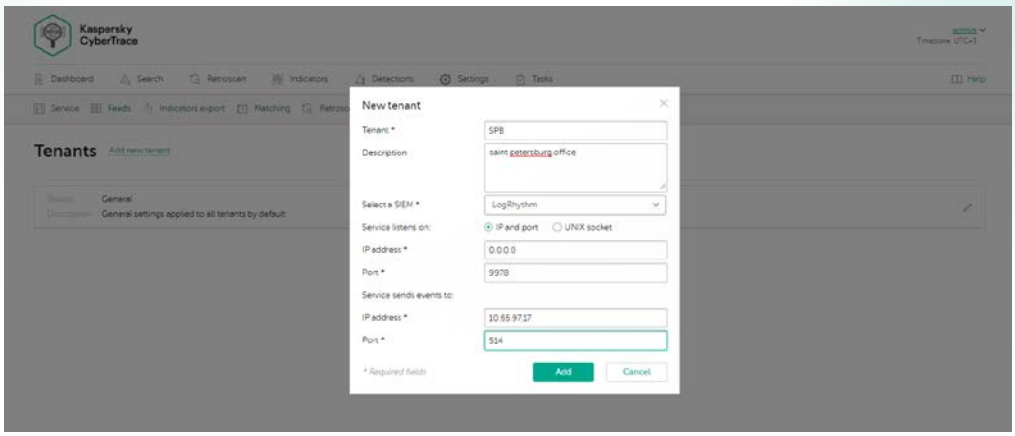
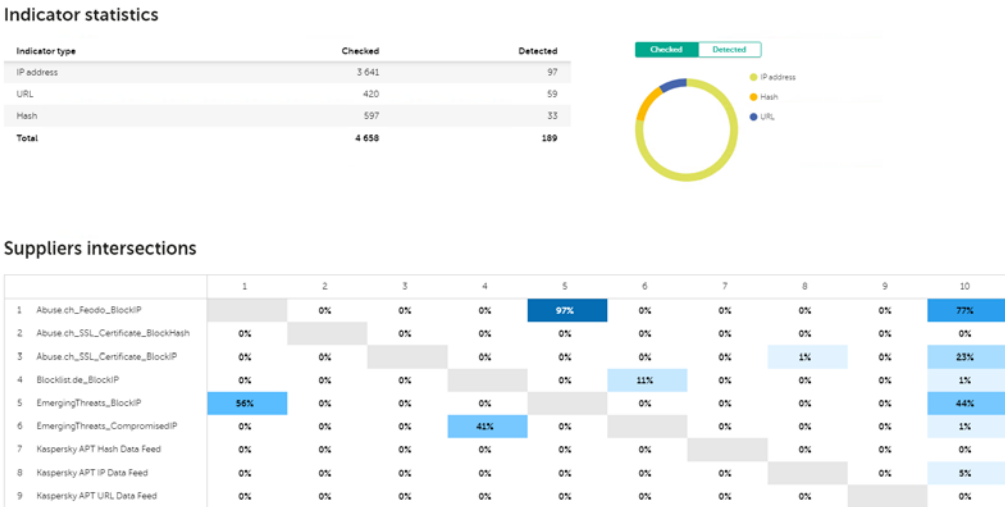


Figura 6. Criação de uma nova locação

- As estatísticas de uso do feed para medição da efetividade dos feeds integrados e a matriz de intersecção de feeds ajudam a escolher os fornecedores de inteligência de ameaças mais valiosos.



Indicator statistics

Indicator type	Checked	Detected
IP address	3 641	97
URL	420	59
Hash	597	33
Total	**4 658**	**189**

Suppliers intersections

		1	2	3	4	5	6	7	8	9	10
1	Abuse.ch_Feodo_BlockIP		0%	0%	0%	97%	0%	0%	0%	0%	77%
2	Abuse.ch_SSL_Certificate_BlockHash	0%		0%	0%	0%	0%	0%	0%	0%	0%
3	Abuse.ch_SSL_Certificate_BlockIP	0%	0%		0%	0%	0%	0%	1%	0%	23%
4	Blocklist.de_BlockIP	0%	0%	0%		0%	11%	0%	0%	0%	1%
5	EmergingThreats_BlockIP	56%	0%	0%	0%		0%	0%	0%	0%	44%
6	EmergingThreats_CompromisedIP	0%	0%	0%	41%	0%		0%	0%	0%	1%
7	Kaspersky APT Hash Data Feed	0%	0%	0%	0%	0%	0%		0%	0%	0%
8	Kaspersky APT IP Data Feed	0%	0%	0%	0%	0%	0%	0%		0%	5%
9	Kaspersky APT URL Data Feed	0%	0%	0%	0%	0%	0%	0%	0%		0%

Figura 7. Matriz de estatísticas de indicador e intersecção de feeds

- A HTTP RestAPI permite que você pesquise e gerencie a inteligência de ameaças. Com ela, o Kaspersky CyberTrace pode ser facilmente integrado a ambientes complexos para automação e orquestração.
- A integração com a plataforma Kaspersky Unified Monitoring and Analysis (KUMA) é compatível, incluindo a integração da IU da Web (IU única).

Embora o Kaspersky CyberTrace e o Kaspersky Threat Data Feeds possam ser utilizados separadamente, quando utilizados em conjunto eles reforçam significativamente as suas capacidades de detecção de ameaças, fortalecendo as suas operações de segurança com visibilidade global das ameaças cibernéticas. Com o Kaspersky CyberTrace e o Kaspersky Threat Data Feeds, as organizações podem:

- Destilar e priorizar de forma eficiente os alertas de segurança
- Reduzir o volume de trabalho de analistas e evitar casos de burnout
- Identificar imediatamente alertas críticos e tomar decisões mais informadas sobre os alertas que devem ser escalados para as equipes de resposta a incidentes
- Criar uma defesa proativa e orientada por inteligência.

Outros recursos do produto:

- Conectores de SIEM para uma ampla gama de soluções de SIEM para visualizar e gerenciar dados sobre detecções de ameaças
- Pesquisa sob demanda de indicadores (hashes, endereços IP, domínios, URLs) para investigação aprofundada de ameaças
- Filtragem avançada para feeds
- Análise em massa de registros e arquivos
- Interface de linha de comando para plataformas Windows e Linux
- Modo autônomo, onde o Kaspersky CyberTrace recebe e analisa os registros de várias fontes, como dispositivos de rede
- E muito mais

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com
Segurança de TI para PMEs: kaspersky.com.br/business
Segurança em TI para empresas: kaspersky.com/enterprise
Portal de inteligência de ameaças: opentip.kaspersky.com

www.kaspersky.com.br

Somos comprovados. Somos independentes. Somos transparentes. Temos o compromisso de criar um mundo mais seguro, onde a tecnologia melhora nossas vidas. Por isso, nós a protegemos. Para que todos tenham acesso às infinitas oportunidades que ela proporciona. Traga o melhor da cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com/transparency

Proven.
Transparent.
Independent.