Kaspersky® CyberTrace

O número de alertas de segurança processados pelos analistas de nível 1 dos Centros de operações de segurança todos os dias está aumentando exponencialmente. Com esse volume de dados analisados, a priorização, a triagem e a confirmação efetiva dos alertas torna-se praticamente impossível. Há muitas luzes piscando, vindas de vários produtos de segurança, e isso faz com que alertas importantes fiquem ocultos pelo ruído e os analistas acabem esgotados. Os SIEMs, o gerenciamento de logs e as ferramenta de análise de segurança que agregam dados de segurança e correlacionam os alarmes relacionados ajudam a reduzir o número de alertas, garantindo a investigação adicional, mas os especialistas de nível 1 continuam extremamente sobrecarregados.

Possibilitando a triagem e análise eficaz de alertas

Com a integração da inteligência de ameaças lida por máquinas atualizadíssima nos controles de segurança existentes, como os sistemas de SIEM, os Centros de operações de segurança podem automatizar o processo de triagem inicial e, ao mesmo tempo, fornecer contexto suficiente para que os especialistas de nível 1 identifiquem imediatamente os alertas que precisam ser investigados ou direcionados para que as equipes de resposta a incidentes (IR, Incident Response) realizem a investigação e a resposta. No entanto, o crescimento contínuo do número de feeds de dados de ameaças e das 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 formatos diferentes e inclui um enorme número de indicadores de comprometimento (IoCs, Indicators of Compromise), dificultando sua compreensão pelos SIEMs ou controles de segurança de rede.

O Kaspersky CyberTrace é uma ferramenta de fusão e análise de inteligência de ameaças que possibilita a perfeita integração de feeds de dados de ameaças com soluções de SIEM para ajudar os analistas a explorar a inteligência de ameaças no fluxo de trabalho de operações de segurança existente com mais eficiência. Ele se integra com qualquer feed de inteligência de ameaças (nos formatos JSON, STIX, XML e CSV) que você queira usar (feeds de inteligência de ameaças da Kaspersky, de outros fornecedores, OSINT ou seus feeds personalizados), com suporte à integração imediata com várias fontes de logs e soluções de SIEM. Comparando automaticamente os logs com os feeds de inteligência de ameaças, o Kaspersky CyberTrace fornece "visibilidade da situação" em tempo real para que os analistas de nível 1 possam tomar decisões mais rápidas e informadas.

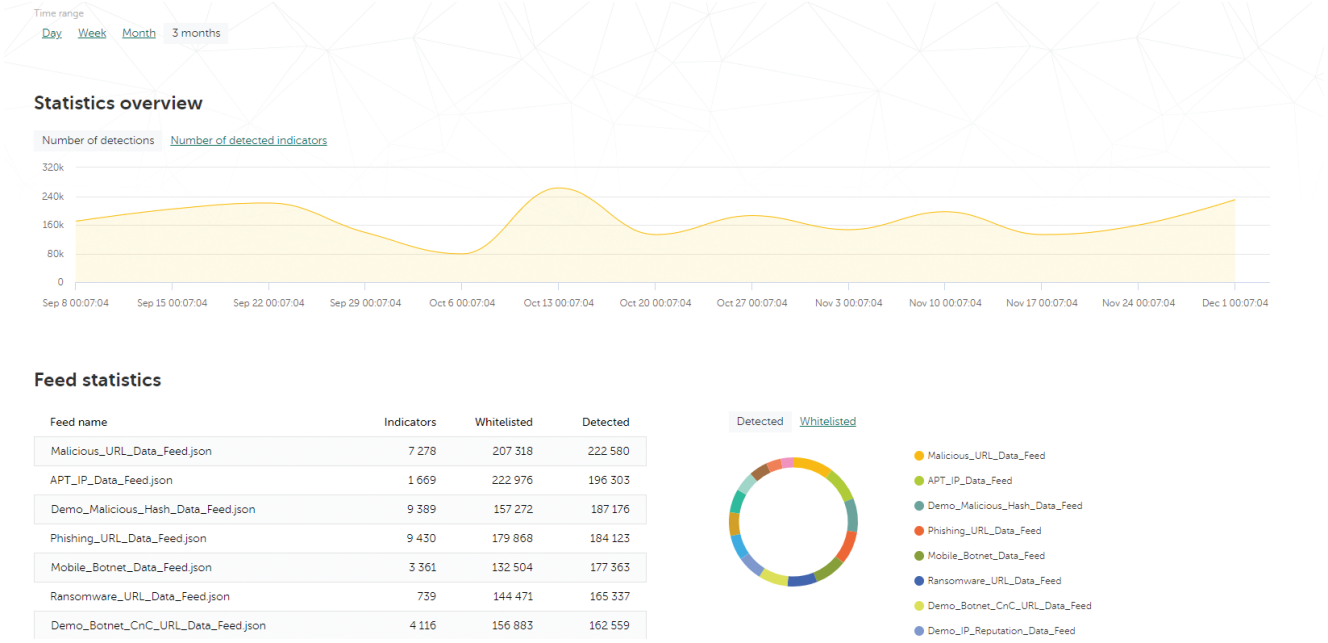


Figura 1. Estatísticas do Kaspersky CyberTrace

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

- Feeds de dados de ameaças da Kaspersky Lab e feeds OSINT de demonstração estão disponíveis prontos para usar
- Conectores para diversas soluções de SIEM para visualizar e gerenciar dados relacionados a detecções de ameaças
- Estatísticas de uso dos feeds para medir a eficácia dos feeds integrados
- Busca de indicadores por demanda (hashes, endereços IP, domínios, URLs) para a investigação aprofundada de ameaças
- Interface Web que oferece visualização de dados, acesso às configurações, gerenciamento de feeds, regras de análise de logs, listas negras e listas brancas
- Filtragem avançada de feeds (com base no contexto fornecido com cada um dos indicadores, incluindo tipo de ameaça, geolocalização, popularidade, carimbos de data e ora e outros) e eventos do log (com base em condições personalizadas)
- Exportação dos resultados da busca correspondentes aos feeds de dados em formato CSV para a integração com outros sistemas (firewalls, IDS de rede e de hosts, ferramentas personalizadas)
- Verificação em massa de logs e arquivos
- Interface de linha de comando para as plataformas Windows e Linux
- Modo autônomo, em que o Kaspersky CyberTrace não está integrado com um SIEM, mas recebe e analisa os logs de várias fontes, como dispositivos de rede
- Instalação em cenários compatíveis com a DMZ, onde precisa ficar isolado da Internet.

A ferramenta usa um processo internalizado de análise e correlação dos dados recebidos, o que reduz significativamente a carga de trabalho do SIEM. O Kaspersky CyberTrace analisa os logs e eventos recebidos, correlaciona rapidamente os dados resultantes com os feeds e gera seus próprios alertas de detecção de ameaças. Uma arquitetura geral da integração da solução é mostrada na figura abaixo:

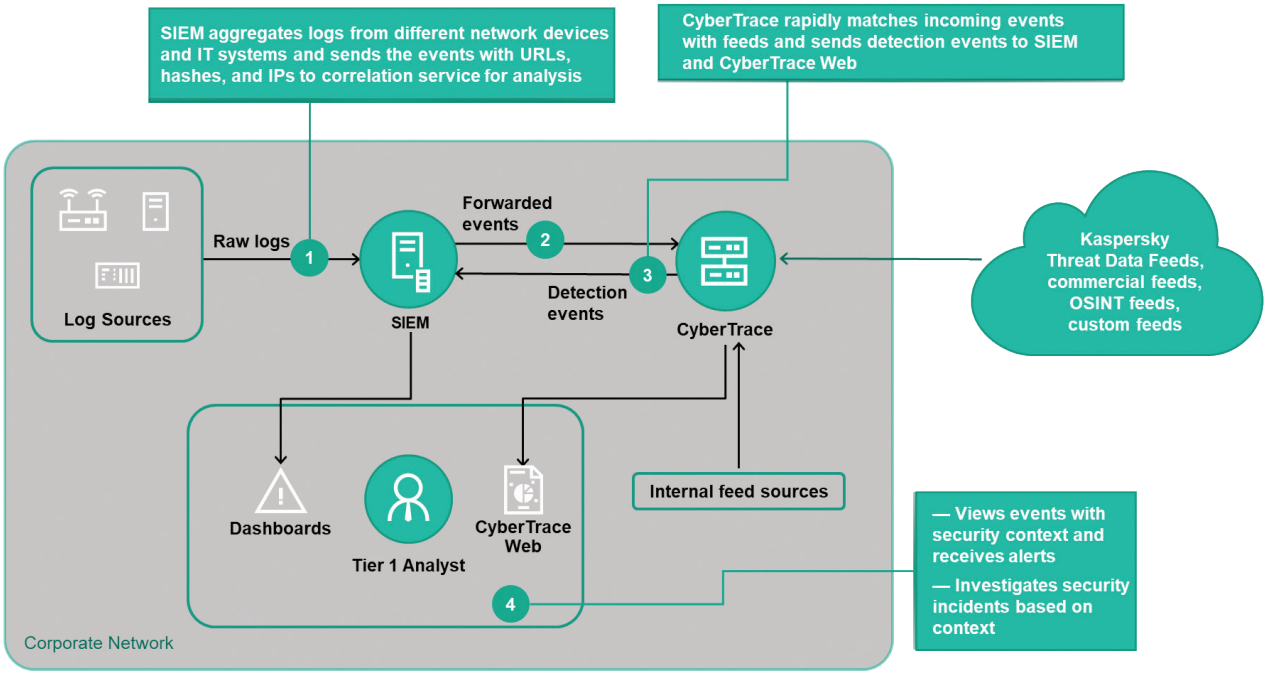


Figura 2. Esquema de integração do Kaspersky CyberTrace

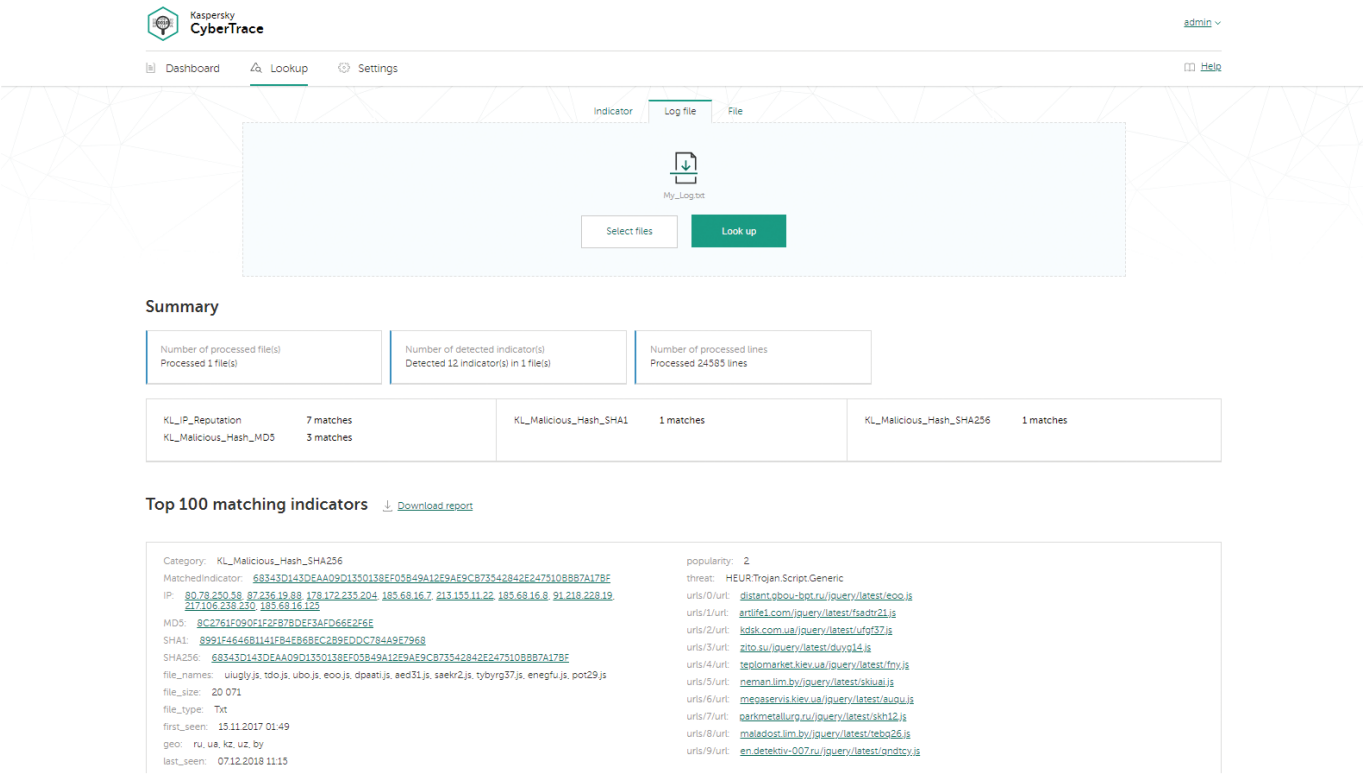
A Kaspersky Lab também oferece um conjunto de feeds de dados de ameaças atualizados continuamente, que podem ser integrados com o Kaspersky CyberTrace para possibilitar a visibilidade global de ameaças, a rápida detecção de ameaças cibernéticas, a priorização de alertas de segurança e a resposta eficiente a incidentes de segurança de informações:

- Feed de reputação de IP – um conjunto de endereços IP com contexto que abrange diferentes categorias de hosts suspeitos e maliciosos

- Feed de URLs maliciosos e de phishing – abrange links e sites maliciosos e de phishing
- Feed de URLs de C&C de botnets – abrange servidores C&C de botnets para desktops e os objetos maliciosos relacionados
- Feed de URLs de C&C de botnets móveis – abrange servidores C&C de botnets móveis
- Feed de URLs de ransomware – abrange links que hospedam objetos de ransomware ou que são acessados por eles
- Feeds da IoC de APTs – abrangem domínios maliciosos, hosts, endereços IP maliciosos, arquivos maliciosos usados por adversários para realizar ataques de APTs
- Feed de DNS passivo (pDNS) – um conjunto de registros que contém os resultados das resoluções de DNS para domínios nos endereços IP correspondentes[1]
- Feed de URLs da IoT – abrange sites que foram usados para baixar malware que infecta dispositivos da IoT[2]
- Feed de hashes maliciosos – abrange os malwares mais perigosos, predominantes e emergentes
- Feed de hashes maliciosos para dispositivos móveis – abrange objetos maliciosos que infectam as plataformas móveis Android e iOS
- Feed de cavalos de Troia P-SMS – abrange cavalos de Troia de SMS, que permitem aos invasores roubar, excluir e responder mensagens SMS, além de cobrar taxas especiais dos usuários de dispositivos móveis
- Feed de dados de lista branca – fornece um conhecimento sistemático de software legítimo a soluções e serviços de terceiros

Os feeds de dados são agregados a partir de uma combinação de fontes unificadas, heterogêneas e altamente confiáveis, incluindo a Kaspersky Security Network e seus mais de 100 milhões de usuários em todo o mundo, que compartilham voluntariamente dados sobre ameaças cibernéticas, nossos próprios rastreadores da Web, o sistema de monitoramento de botnets (monitoramento 24x7x365 de todas as botnets conhecidas, seus alvos e suas atividades), armadilhas de spam, equipes de pesquisa de ameaças e parceiros confiáveis.

Depois, em tempo real, todos este dados agregados são cuidadosamente inspecionados e refinados por meio de diversas técnicas de pré-processamento, como critérios estatísticos, sistemas especializados da Kaspersky Lab (Sandbox, mecanismos de heurística, multi-scanners, ferramentas de análise de similaridade, perfis comportamentais, etc.), validação por analistas e verificação de listas brancas.



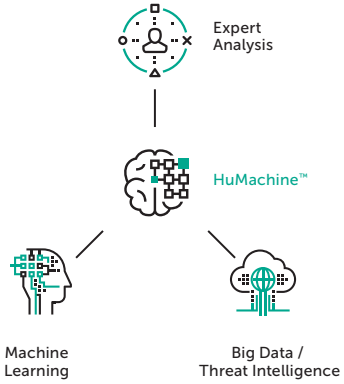
1 Haverá suporte à integração em 2019

Figura 3. Contexto dos feeds de dados de ameaças d

Esses dados contextuais ajudam a entender a 'situação como um todo', confirmando e permitindo o amplo uso desses dados. Dentro de um contexto, os dados podem ser usados de imediato para responder às perguntas quem, o que, onde e quando, que levam à identificação de seus adversários ajudam a tomar as decisões certas.

Embora o Kaspersky CyberTrace e os feeds de dados de ameaças da Kaspersky possam ser usados separadamente, quando usados em conjunto, eles fortalecem significativamente sua capacidade de detecção de ameaças, capacitando suas operações de segurança com a visibilidade global das ameaças cibernéticas. Com o Kaspersky CyberTrace e os feeds de dados de ameaças da Kaspersky, os analistas do Centro de operações de segurança são capazes de:

- Extrair e priorizar enormes quantidades de alertas de segurança com eficiência
- Aprimorar e acelerar os processos de triagem e resposta inicial
- Identificar imediatamente os alertas críticos para a empresa e tomar decisões mais inteligentes sobre quais devem ser direcionados para as equipes de IR



Kaspersky Lab
Cibersegurança para empresas: **www.kaspersky.com.br/enterprise**
Notícias sobre ameaças cibernéticas: **www.securelist.com**
Notícias sobre segurança de TI: **www.kaspersky.com.br/blog**

#truecybersecurity
#HuMachine

www.kaspersky.com.br